Why a secure enterprise workspace is the best approach for mobile productivity

Introduction

Across industries, many organizations recognize the important benefits of providing tools for mobile productivity. With anytime, anywhere access to enterprise information and resources, employees can be more productive and responsive to customers and colleagues. In many cases, they work more hours: A recent study commissioned by Dell showed that employees, on average, work more than 351 extra hours annually when they use mobile devices.[1]

Employees also enjoy greater work flexibility. Having the ability to read emails while waiting for the train home or taking a call while running a midday errand can significantly improve the work/life balance.

While some organizations are deploying corporate-owned devices to foster mobile productivity, others are allowing employees to use personally owned devices through a bring-your-own-device (BYOD) program. BYOD programs can help organizations avoid the costs of purchasing devices and enable employees to use the devices they prefer.

You need the manageability to efficiently control enterprise information even as that information is being accessed from a broad variety of devices across the enterprise.

The benefits of mobile productivity are clear. But with a wide variety of mobility solutions available today, selecting the right technological approach is critical for addressing security, manageability and configurability challenges. You need an approach that can help maintain tight security of enterprise information and networks. In addition, you need the manageability to efficiently control enterprise information even as that information is being accessed from a broad variety of devices across the enterprise. Finally, you need an approach with the configurability for delivering the precise tools that individuals and groups need, so you can maximize the benefits of mobility.

A secure enterprise workspace approach can address these requirements. With the right workspace solution, you can create a secure, managed environment that has the configurability to deliver the particular tools and resources needed by individuals and groups.

Approaches to enabling mobile productivity

There are numerous possible approaches to enabling mobile productivity, each with potential advantages and disadvantages.

Anything goes: You could simply allow employees and contractors to use their own personal devices with whatever personally owned and installed applications they desire. But doing so would expose enterprise data while it resides on the devices and while it is in motion between devices and the corporate network. Employing individual security solutions such as a virtual private network (VPN) could help protect data in motion, but enterprise data would still be vulnerable if a device is lost or stolen.

Web-based applications: With web-based applications, employees need only a web browser to use a web-based version of their email application, customer relationship management (CRM) system or other software. The web-based approach might work well if a web-based version of an application already exists. Developing a web-based version of software, however, can be costly and time-consuming. For users, web-based applications can be difficult to use on smartphones and any other devices with small screen sizes unless they have been optimized for mobile use.

Fully managed devices: You might decide to control and manage the entire operating environment. This approach provides tight security and is commonly used for corporate-issued devices. Users, meanwhile, have a familiar experience: They use mobile apps or desktop applications just as they would normally. This approach can be costly, however. Your organization would need to purchase the devices (if you decide to provide them) and pay wireless carrier costs. Moreover, the user must sacrifice privacy: You could theoretically access any data on the device, including your users' personal email, texts, pictures and so on.

An alternative approach: The secure enterprise workspace

A secure enterprise workspace is an alternative approach that can provide some distinct advantages. It is a single, secure environment on a smartphone, tablet or laptop where users can access multiple applications and enterprise resources. The implementation of the workspace might vary according to the device type, operating system, deployment method and other factors, but in each case, the workspace keeps enterprise applications and data separate from the applications and data of the host system.

A workspace approach can be beneficial for BYOD programs since the workspace keeps enterprise applications and data distinct from personal applications and data. You can prevent enterprise data from being moved or copied between the workspace and the personal environment, and to external devices and media. You can also prevent

malware and viruses acquired in the personal environment from affecting your enterprise network.

Employees benefit from workspaces as well. Implementing a workspace approach enables them to use their preferred, personally owned devices, which can help boost satisfaction, efficiency and productivity. They no longer have to carry separate enterprise and personal devices with them. And they do not have to adapt to new ways of working, which might be required if they must use an enterprise-issued device or another technology approach to mobile productivity.

In addition, workspaces help preserve employee privacy. Employees can use their personal devices without concern that their employer is monitoring or controlling their personal activities. With the workspace approach, IT manages only the workspace, not the personal environment. The enterprise IT department won't access personal email, texts, photos, browser history or anything else in the personal environment.

A workspace can also help protect highly regulated data, especially when you use a cloud-hosted desktop virtualization model for deploying the workspace.

With a desktop virtualization approach — specifically a virtual desktop infrastructure (VDI) or Remote Desktop Session Host solution — you keep the applications and desktop environment running in the data center. There is no enterprise data kept on the devices. Users gain access to a full desktop environment or individual remote applications from any device.

Dell offers secure enterprise workspace solutions that help your organization improve mobile productivity while meeting enterprise requirements for security, manageability and configurability.

- **Dell Mobile Workspace:** Provides a secure enterprise workspace on Apple® iOS and Google® Android™ smartphones and tablets.
- **Dell Desktop Workspace:** Enables you to provision a complete corporate Windows image in a secure workspace on laptops running Windows or Mac® OS X® and Windows Pro–based tablets.
- **Dell Wyse vWorkspace:** Offers a blended model of VDI and terminal server technology that lets users access a workspace from a wide range of devices — including smartphones, tablets, laptops and desktops — while keeping enterprise applications and data secure in the data center.

There are numerous possible approaches to enabling mobile productivity, each with potential advantages and disadvantages.

Dell secure enterprise workspace solutions support a wide range of smartphones, tablets and laptops.

A workspace approach can be beneficial for BYOD programs since the workspace keeps enterprise applications and data distinct from personal applications and data.

Maintaining tight security

Security is a top concern among organizations as they implement mobility programs and BYOD initiatives, and tight security is one of the primary advantages of a workspace approach. Workspace solutions can use a combination of security technologies to protect data and enterprise networks.

Data-loss protection (DLP): DLP capabilities restrict data movement between the enterprise environment and the host environment. Intellectual property, confidential customer information, enterprise financial information and any other sensitive enterprise data stays secure and controlled by the enterprise.

With Dell workspace solutions, you can specify which particular activities you want to prohibit. For example, you might prevent users from saving attachments from enterprise emails into the personal environment, printing corporate documents on a personal printer, or copying files to an external USB drive or DVD.

In some cases, you might decide to allow data movement between the secure enterprise workspace and the personal environment. You might allow a smartphone user to copy an address from a company email to a personal map app, for example. You might also allow a graphic designer to begin a logo project in the office, transfer the project to a secure USB drive, and then move files to a Desktop Workspace on a personal laptop to continue working on the project while traveling or at home. Dell workspace solutions let you define the group and individual policies for moving data.

Encryption: Encryption technology can help ensure that data stays protected when it resides on a device (as with Mobile Workspace and Desktop Workspace) and when it travels between the device and the enterprise network (as with all three Dell workspace solutions). Mobile Workspace applies AES-256–level encryption automatically to all data within the workspace. Desktop Workspace allows you to apply AES-256, AES-128 or no encryption. You might choose no encryption if you plan to incorporate an existing encryption solution into the Windows image you deploy within the workspace. All three Dell workspace solutions use the Secure Sockets Layer (SSL) protocol to protect data in motion as it travels between devices and enterprise servers.

Secure remote access (SRA): SRA capabilities help protect data and networks as users connect to enterprise networks and resources. You can authorize access to resources on a per-user or per-device basis. You can also require validation of the certificate status and OS version, and confirm that devices have not been jailbroken or rooted. Dell secure enterprise workspace solutions incorporate multiple SRA/VPN solutions, such as Dell Secure Mobile Access (SMA), to help ensure the security of remote connections with the enterprise network.

Identity and access management (IAM): IAM capabilities help ensure that only authorized individuals can access enterprise information and systems. Effective IAM can help you prevent intrusions resulting from incorrect, abused or compromised access credentials.

Auto-lock, auto-kill and remote wipe: While Wyse vWorkspace keeps data in the data center, Mobile Workspace and Desktop Workspace store enterprise data securely on devices. But what happens if a device is lost or stolen, or if an employee leaves the organization? These solutions allow you to set policies that automatically lock a user out of a workspace after a certain number of days or weeks of inactivity. You can also use "auto-kill" capabilities to automatically wipe the data from the workspace after an additional span of inactivity. If an employee leaves the organization, or a contractor's term ends, you can remotely wipe the workspace — without affecting personal information on the device.

Dell secure enterprise workspace solutions centralize management.

Next-generation firewalls: You can implement additional layers of protection by deploying workspaces in conjunction with next-generation firewalls such as Dell SonicWALL next-generation firewall solutions, which scan every packet entering and exiting the network.

Manageability

A secure enterprise workspace can provide the manageability and control you need to make sure security policies are appropriately enforced, streamline administrative functions and maintain compliance with government and industry regulations. If you allow employees to use their own applications outside of a workspace (the "anything goes" approach), you might be putting enterprise information at risk while significantly increasing the complexity of management, support and compliance. By contrast, a workspace approach allows IT to focus solely on the workspace. Administrators can more easily control interactions with enterprise applications, data and other resources. The result is better security and compliance with less complexity.

Dell workspace solutions can help address manageability requirements through policy-based management, centralized administration and reporting capabilities.

Policy-based management: With the Dell workspace solutions, you can set custom policies for a wide range of security capabilities. For example, you can prohibit users from moving enterprise data to external USB drives; establish the number of password attempts each user is allowed before he or she is locked out of the workspace; set the amount of elapsed time between logins before workspace data is wiped from a device; and so on. You can apply established policies to specific groups, particular individuals or your entire user base. With Wyse vWorkspace, you can also apply policies to IP subnets, device names, organizational units or Boolean-based combinations of them all.

Centralized administration: Dell workspace solutions centralize administrative functions to help streamline management of workspaces, whether they are running on employee- or enterprise-owned devices. With the Desktop Workspace console, for example, you can manage the Windows images you deploy, create and manage groups, set and apply all security policies, and access reports — all from the same place. You can also use the Desktop Workspace console alongside tools such as Microsoft System Center Configuration Manager (SCCM). The Mobile Workspace console similarly lets you manage groups, policies and reports while also enabling you to provision optional productivity services. From the Wyse vWorkspace console, you can create groups, manage security capabilities, automate tasks, generate templates for provisioning, manage gold images and more.

A workspace can also help protect highly regulated data, especially when you use a cloud-hosted desktop virtualization model for deploying the workspace.

User work functions also help determine which workspace solution (or solutions) are the right ones to deploy for particular individuals and groups.

VDI monitoring capabilities built into Wyse vWorkspace help accelerate diagnostics and problem resolution.

Reporting capabilities: In addition to securing sensitive information, you need to comply with industry and government regulations and be prepared to demonstrate compliance to regulators. Dell workspace solutions provide reporting and auditing capabilities that help streamline the process of proving compliance. You can run reports that show all users and devices that have access to regulated data. You can even create a group for each type of regulated data and report on each group separately. In addition, you can log file operations and produce an audit trail of a user's activities with regulated data.

Configurability

A secure enterprise workspace approach can deliver a high level of configurability. You can configure the workspace in a variety of ways to meet the specific productivity needs of groups and individuals without adding significant complexity.

For example, with Desktop Workspace, you can create one or many distinct Windows images. An operations group might need to use inventory software to run on Windows Pro–based tablets, while the marketing team might need presentation and graphic design software for its desktops and laptops. You can build distinct Windows images and then manage them easily from the Desktop Workspace console. Adding software to an existing image, pushing updates and provisioning new users are straightforward processes.

Similarly, Wyse vWorkspace allows you to create multiple golden workspace images. You can configure images of various sizes, using a range of operating environments and applications.

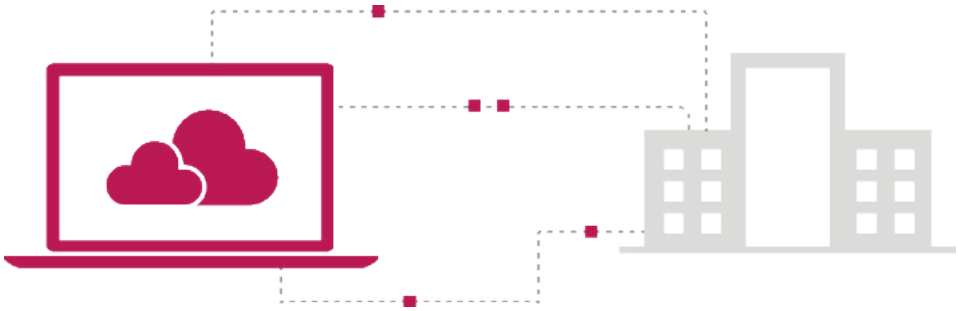
Mobile Workspace provides a set of core, built-in productivity apps within the workspace, including email, calendar, contacts, a secure browser and a secure file explorer. But you can also add productivity services as needed by individuals and groups. For example, mobile sales team members or executives might need Dell Business Phone, which provides a complete, separate business phone service within the secure workspace. Dell Business Phone offers a distinct business phone line, phone number and text messaging service, plus optional capabilities such as a conference bridge and call recording. You can also add Box for Dell, which provides an enterprise-grade content collaboration solution accessible from within the workspace.

You enable these productivity services for particular users or groups and manage all the apps and services from the centralized Mobile Workspace console. Once you've acquired the appropriate licenses, you simply check boxes to incorporate these apps for selected users and groups. Adding these services is easy and requires no work from users.

Selecting from multiple deployment methods

A secure enterprise workspace can be implemented in multiple ways depending on user and enterprise needs. Dell workspace solutions enable you to support a full range of device types, operating systems, connectivity scenarios, work functions, security requirements and other deployment preferences.

Device type and operating system: Will your employees need to access enterprise resources from a smartphone, tablet or laptop? Mobile Workspace is designed for smartphones and tablets, while Desktop Workspace is designed for laptops and Windows Pro–based tablets. Wyse vWorkspace can support a wide array of devices and operating environments, including any system and operating environment that can run an HTML5-capable web browser. The Wyse vWorkspace approach is generally best suited for laptops and tablets with larger screen sizes rather than smartphones



A cloud-hosted desktop virtualization deployment model helps highly regulated data remain secure by keeping it in the data center.

or small-screen tablets. In many cases, organizations will deploy more than one type of workspace to support the myriad devices and use cases across the enterprise.

Connectivity: Mobile Workspace and Desktop Workspace support offline productivity. Workers can continue to access all applications and data even when there is no network connection or a low-bandwidth connection. The workspace automatically synchronizes with enterprise servers when connectivity is re-established. With this capability, Mobile Workspace and Desktop Workspace might be the right solutions for employees who are frequently on the move or working in remote areas with spotty network connectivity.

Wyse vWorkspace requires consistent network connectivity to provide access to applications or a desktop. However, the solution has built-in tools to eliminate latency in remote environments, so users can use this solution even when bandwidth is not optimal.

Work functions: User work functions also help determine which workspace solution (or solutions) are the right ones to deploy for particular individuals and groups. For example, you might deploy Mobile Workspace to mobile workers who need to access only email, calendar, contacts and business phone capabilities from mobile devices. Desktop Workspace would be the right solution for employees who require a full Windows environment with access to several enterprise applications. Wyse vWorkspace might be the right fit for users who need to access a Windows or Linux® environment or specific enterprise applications from a wide array of devices, from laptops and desktops to tablets and smartphones.

Security and compliance: All Dell workspace solutions offer tight security and can help organizations achieve compliance with rigorous regulatory requirements. To meet the strictest regulations, organizations can keep enterprise data locked down in the data center with Wyse vWorkspace.

Conclusion

As your organization launches or expands its mobility program, you need technology that gives users the tools they need for boosting productivity while also securing enterprise information and controlling administrative complexity. A secure enterprise workspace can offer a compelling approach that delivers exceptional security, manageability and configurability. Capitalize on the benefits of the secure enterprise workspace approach and meet a wide range of user and enterprise requirements with Dell secure enterprise workspace solutions.

Learn More

Dell Mobile Workspace: software.dell.com/products/mobile-workspace/

Dell Desktop Workspace: software.dell.com/products/desktop-workspace/

Dell Wyse vWorkspace: Dell.com/wyse/vWorkspace

Dell Mobile Solutions: Dell.com/mobility

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

[1] *IDG Research Services survey conducted in September 2014.*

February 2015