Software

Is a secure workspace approach right for you?

Recognize the potential benefits and identify the best use cases for a secure workspace approach to providing enterprise software and resources

Today, there are multiple options for providing employees with the software and other enterprise resources they need to do their jobs. Which approach is the right one for each of your use cases? In each situation, the best approach should balance employee expectations, business goals, IT requirements and security needs.

A secure enterprise workspace can offer the right approach for a variety of use cases. With a secure workspace solution, you can quickly provide a complete enterprise environment, with all necessary software, in a workspace that is isolated from the host environment. Whether employees are using personally owned or corporate-owned laptops, tablets or smartphones, they can access the resources they need and continue to work even when they are offline. The workspace also helps simplify provisioning and management of enterprise environments while helping to maintain tight security.

Meet employee expectations

A secure workspace solution can address employee expectations for fast, easy, anytime access to necessary software and enterprise resources. It can also deliver a consistent and responsive experience across a variety of device types, regardless of who owns them.

Employees can download, install and configure the necessary software with minimal help from IT.

Fast, self-service installation: With a workspace solution, employees can get to work fast. In most cases, employees can download, install and configure the necessary software with minimal help from IT. Whether starting a new job or provisioning a new computer, employees can avoid a potentially long queue for IT assistance.

BYOD/BYOPC: The secure workspace approach supports the bring-your-own-device (BYOD)/bring-your-own-PC (BYOPC) model. If your organization allows it, employees can run workspaces on their personally owned laptops, tablets and smartphones. Employees gain the flexibility to use their preferred computers and mobile devices.

At the same time, employees can be confident that the workspace software won't alter personal configurations or tap into any personal data — the workspace is isolated from the host environment. IT does not need to access personal information or change any system settings.

Responsive, consistent experience with required software: Within the workspace, IT can provide a full range of required software as well as secure access to enterprise resources, including file-sharing environments. With the right workspace solution, your organization can even support commercial, cloud-based storage solutions — all files accessed within the workspace are encrypted so data remains protected.

Because the workspace and its applications run locally on a laptop, tablet or smartphone, employees enjoy strong application performance and a responsive experience. The right solution also provides a consistent experience across devices — employees do not have to learn multiple interfaces to access the same enterprise resources.

Enterprise support: While employees gain the flexibility to use a wide variety of devices, including personally owned devices, they also benefit from IT management of enterprise applications. Your IT group can help ensure that the operating system and all applications are configured correctly and updated in a timely manner. Employees no longer have to worry about those IT tasks to do their work.

Employee-controlled upgrades: If you use a secure workspace solution in conjunction with a BYO program, the workspace will allow employees to move to new devices on their own schedule. They can purchase a new laptop or upgrade to the latest smartphone without having to get approval from IT. As they move from one device to another, employees can continue to use the same workspace. This capability will be particularly useful as more mobile device carriers introduce short-term lease programs that encourage users to upgrade devices more frequently than in the past.

Offline productivity: Importantly, a secure workspace approach lets employees maintain productivity even in situations with poor or no network connectivity. While virtualized desktop infrastructure (VDI) solutions and web-based applications require a continuous connection to the corporate network, the secure workspace allows employees to continue to work on applications within the workspace even when they are not connected to the company network or even the internet — information is synced when connectivity is restored.

Deliver IT and business benefits

A secure workspace offers several benefits to IT and the business. IT can more easily keep enterprise information safe while reducing administrative burdens. The business can enable anywhere, anytime productivity for employees while controlling costs.

Tight security: Delivering an enterprise workspace that is isolated from the host environment helps provide a high level of security. Unless you specifically allow it, employees are unable to transfer data between the host environment and the workspace. All work that employees do within the workspace is encrypted.

The right solution provides secure access to corporate resources and enables you to set granular settings and access policies to protect enterprise networks. You can help ensure employees have access to the resources they need without giving them any more than they need to do their jobs.

With a workspace solution, you also retain the ability to remotely patch and update software in the workspace, helping to prevent security breaches. If a computer is lost, an employee leaves the company or a contract project

With a secure workspace solution, IT can more easily keep enterprise information safe while reducing administrative burdens.

For the business, the primary benefit of the secure workspace approach is improved employee productivity.

comes to an end, you can automatically lock the workspace or remotely wipe enterprise data from the workspace.

Streamlined management: The workspace approach also helps simplify IT management. For client systems, you can manage a single golden desktop image of the enterprise environment — with the operating system, all necessary productivity applications, mobile access software and more — instead of trying to manage numerous unique combinations. Any software patches and updates can be done just once.

A secure workspace with self-service capabilities can also accelerate provisioning of new systems and devices. Employees do not need to request IT assistance or install and configure applications. All of the required software is integrated and optimally configured as part of a corporate image (in the case of client systems) or a mobile app. Self-service capabilities help new employees and contractors get to work quickly while allowing IT administrators to focus on other tasks.

Ongoing IT support is also easier. You need to manage only a single software environment and a single set of software applications. If your organization offers BYOD or BYOPC, you can avoid having to support multiple device types and platforms.

Improved productivity: For the business, the primary benefit is improved employee productivity. A secure workspace solution gives employees anytime, anywhere access to the software and resources they need to work. With the flexibility to use a wide range of devices (including personally owned devices), employees can work whether they have a laptop, tablet or smartphone within arm's reach.

Because the workspace provides offline productivity, employees can continue working even when they are on a plane or in a location where network connectivity is poor.

Controlled costs: A secure workspace approach can help control costs. For example, you can launch or expand a BYO program and provide a secure enterprise workspace for those personally owned systems instead of buying new systems for employees and contractors. You can also reduce the need for multiple corporate-owned systems. For example, you can avoid purchasing two distinct computers for software developers: one for engineering applications and another for corporate functions. With the workspace, those environments can run side by side on the same computer.

Secure workspace solutions do require some infrastructure in the data center. However, with the right solution, you can enable IT management and protect enterprise data while minimizing the need to buy and operate numerous servers and storage systems.

Identify use cases for the secure workspace

There are several use cases for which a secure workspace offers a compelling solution.

Task workers: In many organizations, a large portion of employees are task workers: people who typically use common, industry-standard software to accomplish a variety of tasks, such as interacting with customers, producing marketing materials or taking care of billing and accounting. These task workers might use personally owned devices instead of or in addition to corporate-owned devices. They might work in the office as well as at home or on the move — and they might not always have reliable network connectivity.

A workspace solution offers an easy way for task workers to access enterprise software and resources on a wide array of devices, from corporate-owned laptops to personally owned tablets. Your IT group can provide all productivity software that they need within a workspace that is isolated from the host environment. Because workspaces allow applications to run locally, these employees can continue to be productive even when they do not currently have internet connectivity.

Contract employees: Deploying a workspace can also be the right approach for providing contract employees with enterprise resources. By using one, you can avoid providing corporate-owned systems to contractors. You can also eliminate potential software compatibility problems if contractors are using personally owned devices but have a different operating system or different software versions than your organization uses. Simply enable contractors to download and install software onto their existing systems. They can use laptops, tablets and smartphones that are personally owned or owned by their own organization. When the contract term is over, you can revoke access to corporate resources and/or remotely wipe any enterprise data from contractors' systems.

Mergers and acquisitions: If your organization merges with or acquires another organization, you might suddenly find that you have hundreds or thousands of new employees for which you need to provide access to your corporate resources. With the workspace approach, you can avoid the time and costs of providing and provisioning new, corporate-owned systems. New employees can download and install the necessary software and start working right away. As with contractors, these employees can continue to use existing laptops, tablets and smartphones, whether they are owned by the employees or by the organization that is being integrated into yours.

Offshore developers: Offshore software development teams are also good candidates for workspace solutions. Organizations that use offshore teams need to provide access to code repositories and test and development environments without jeopardizing the security of intellectual property and enterprise systems. With a workspace, you can provide offshore teams access to company resources while maintaining control over the enterprise workspace and sustaining tight security. If the contract ends or if you decide to use different developers in the future, you can easily reassign development services to another supplier.

Recognize use cases for other approaches

A secure workspace approach is not the best fit for all use cases. For example:

Call-center employees: The employees who work in large, corporate-run call centers are not the best candidates for workspaces. Typically, these employees use corporate-owned systems: IT installs and manages all the software in the environment. The corporate-owned systems remain in the call center, where employees have consistent network connectivity. For this use case, organizations might benefit from a native application approach or a VDI solution, which helps ensure that all data remains secured in the data center.

Because workspaces allow applications to run locally, employees can continue to be productive even when they do not currently have internet connectivity.

Dell EMM is a comprehensive mobile enablement solution that allows you to secure and manage your enterprise workspaces and devices — regardless of who owns those devices.

Employees using data-intensive applications: Employees using data-intensive applications, such as computer-aided design (CAD)/computer-aided manufacturing (CAM) software, are often better served with other approaches to providing enterprise resources. These workers need to access and work with very large data sets that are stored in the enterprise data center (or in a departmental environment). Running the software locally — within a workspace or using a native-application approach — would require transferring those large volumes of data back and forth between the employee's computer and the data center. Even with a reliable, high-bandwidth network, that data transfer process can be slow and costly. VDI solutions or similar approaches that leave data in the data center might be preferable.

Implement a secure workspace solution with Dell Enterprise Mobility Management (EMM)

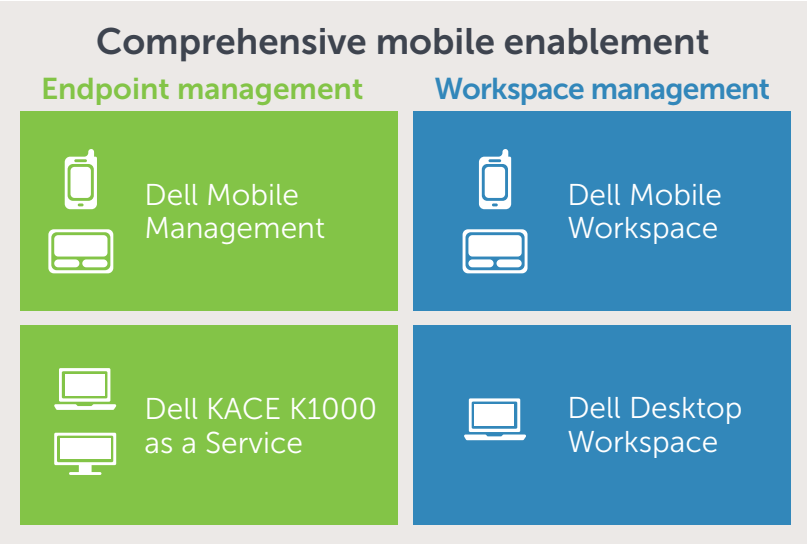
Address employee, business, IT and security requirements with Dell Enterprise Mobility Management (EMM). Dell EMM is a comprehensive mobile enablement solution that allows you to secure and manage your enterprise workspaces and devices — regardless of who owns those devices. Built with industry-leading security and management technology, Dell EMM provides an encrypted, secure workspace for personally owned or corporate-owned/shared laptops, tablets and smartphones. The workspace separates personal data and apps from enterprise data and apps. Employees can use their personally owned devices to run their own apps and keep personal data on the device without it commingling with enterprise or regulated data.

Dell EMM provides two secure workspace components:

- **Dell Mobile Workspace:** Self-service capabilities for mobile devices enable employees to simply download and install a single app whether they are using Apple® iOS or Google® Android™ phones or tablets. Providing a workspace for Android devices opens new possibilities for many organizations that might have previously limited support to iOS devices because of security concerns with the Android platform. Built-in email, calendar, contacts, mobile browser and file explorer applications give employees the essential productivity tools they need, right away.
- **Dell Desktop Workspace:** For laptops or Windows Pro-based tablets, your IT group can create and deliver a Windows-based corporate image with all necessary applications on Windows and Mac OS® systems. The processes of building, delivering and managing laptop workspaces easily integrate with existing IT infrastructure and processes.

No matter what types of devices your employees use, they can keep working even when they do not currently have an active network connection. They simply save their work; data syncs automatically when they reconnect.

Mobile Workspace and Desktop Workspace let your IT group manage apps and content, set policies and remotely wipe enterprise data from the enterprise workspace. Enforcement of data-loss protection (DLP) policies — including copy/paste restrictions, data-sharing restrictions, password protection, data encryption and auto lock/wipe functions — helps keep enterprise data secure and isolated from an employee's personal space. Reporting capabilities enable your IT administrators to conduct asset inventory for workspaces in the same way as if these workspaces were physical devices.



Dell EMM is a comprehensive solution that provides secure workspaces for smartphones, tablets and laptops while also providing extensive endpoint management capabilities. Cloud-based endpoint management is offered through Dell Mobile Management and Dell KACE K1000 as a Service.

Beyond workspace management and provisioning, Dell EMM provides extensive management capabilities for a wide array of corporate-issued and BYO devices, including smartphones (iOS, Android), tablets (iOS, Android, Windows Pro), laptops and desktops (Windows, Mac, Linux®).

Dell EMM integrates all of these common functions:

- Endpoint systems management (ESM)
- Mobile device management (MDM)
- Mobile application management (MAM)
- Mobile content management (MCM)
- 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

Balance employee, business, IT and security requirements

Whether you issue corporate-owned systems to employees or enable them to use personally owned devices for work, there are multiple ways to ensure they have the required software and resources to do their jobs. You might find that a secure workspace solution offers the right approach for several use cases. By using Dell EMM as your secure workspace solution, you can deliver the responsiveness and flexibility that employees need for anytime, anywhere productivity while maintaining security and reducing IT complexity.

Learn more

Dell Enterprise Mobility Management (EMM):
Dell.com/EMM

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

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

Dell Mobility Solutions:
www.dellmobilitysolutions.com

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

Dell EMM provides extensive management capabilities for a wide array of corporate-issued and BYO devices.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology — delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our website for regional and international office information.

July 2014