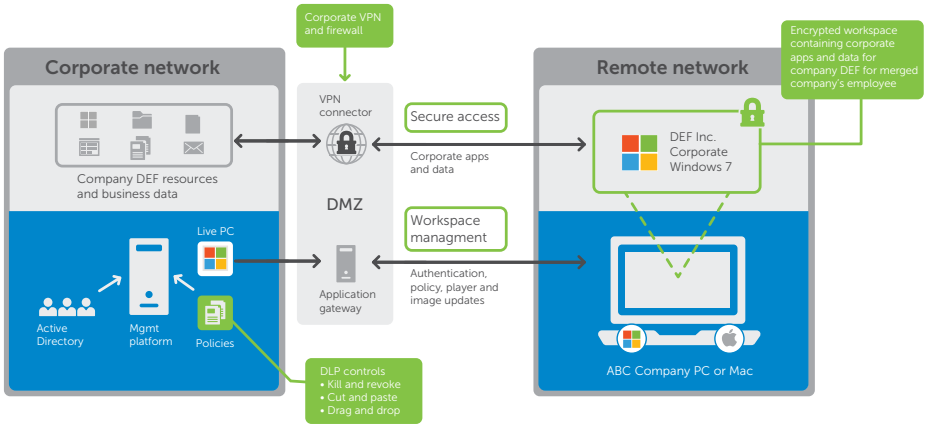
# Desktop Workspace for mergers and acquisitions

Execute a seamless IT infrastructure integration to help ensure business growth

Merging two distinct entities into one productive organization is fraught with challenges. A key to achieving business goals is the successful integration of IT systems and processes. You must rapidly deliver consistent desktop images with access to the right applications and data to every employee.

Your first challenge is to determine the fastest path to integrate applications and data across the merged business. Integration of business functions and the applications that support them takes time to plan, develop and execute. Taking the applications and data from each business and delivering all of it to the combined workforce can be expensive and impractical. Each business could be on a different Microsoft® Windows® operating system release with fundamentally different applications, virtual private network (VPN) clients, file shares and Microsoft Active Directory® services. You need to deliver the applications and data required to serve the unique functions of both businesses, along with a solution path to a combined, standardized application and data set for the merged enterprise.

Dell™ Desktop Workspace — a component of Dell Enterprise Mobility Management (EMM) — can help ease the critical IT transition necessary after a merger or acquisition. This solution's secure, managed container delivers a corporate Windows image with low-friction integration with your IT




Benefits:

- Quickly provide employees with the applications and data they need in the merged business
- Boost end-user productivity and improve satisfaction
- Prevent data leaks and loss of intellectual property with a secure enterprise container
- Enable productivity offline and even in low-bandwidth environments
- Simplify image management, updates and data wiping
- Provide policy-based, secure corporate access regardless of operating system or network
- Streamline administrative tasks with unified management control

Learn more at software.dell.com/products/desktop-workspace

Merging two distinct entities into one productive organization can be fraught with challenges. Timing is critical and IT is a critical piece of the puzzle.

infrastructure and processes. Create, manage and deploy new images to every employee's system in minutes or hours — not days or weeks. This solution gives you critical capabilities for enhancing end-user productivity and helping to ensure the success of the new organization.

With Desktop Workspace, you can provide Windows images that include the applications and data required for individual groups of business users to do their jobs in the merged business. If a set of Company A's applications need to be provided to employees from Company B, this solution can be the tool to create, deliver and manage the image and applications on users with Company B's systems. As you create an integrated set of applications for the business, you can use Desktop Workspace to create, deliver and manage the combined image, regardless of which company's base image is on the user's system. This containerized solution eliminates the need to reimage systems across the business.

If one company brings a base of Apple® Mac® computers to the combined business, Desktop Workspace can provide the Windows image and applications required for the merged business on those users' Macs. To make it easier to add management of the secure, containerized image to the systems management practices of the merged business, this solution can integrate with existing Windows software management tools such as Microsoft System Center Configuration Manager.

## Container management for mergers and acquisition

Desktop Workspace is based on the fundamental premise that data and applications, not devices, have the real value and require management. As networks become the dominant computing infrastructure, data now exists abstracted from the devices. Users can access data across locations, devices and even networks, while you gain centralized control of that data while facilitating user access. With Desktop Workspace, you can create a highly elastic enterprise perimeter where all your critical data and applications can be encrypted and safely delivered to any device as a simply managed container.

The container runs a corporate Windows image, including the OS, applications and data. With this solution, your organization can give employees access to business operations systems, financial and accounting data, business and product plans, customer service and support systems, the company email system, the corporate directory and more. The container is physically and logically separate from the OS, applications and data on the user's system. You can manage the container without affecting the user's personal applications and data.

With Desktop Workspace, you manage the container and the Windows image with a robust set of policies. You can create an image and apply a set of policies as part of the deployment process. If you need to adjust management policies to be more restrictive or permissive, you can dynamically apply new policies to the user's container.

For example, you can dynamically apply kill and revoke policies to protect corporate applications and data within the container. These policies provide critical controls if a system is lost or stolen, or a security breach is suspected. The revoke policy prohibits a user from accessing the corporate image in the container. The image and data still reside on the user's system, but the user can't access the image and data until an IT administrator reauthorizes them. kill allows the IT administrator to destroy the container and its contents. If employees leave the company, administrators can use the kill policy to remove all enterprise applications and data from the system.

Desktop Workspace also provides policies that prevent corporate data — such as customer information, business plans, financial data or other IP — from being exposed through applications on the employee's system. For example, you can apply a policy to prevent an employee from copying and pasting data between corporate applications and personal applications. You can also apply a policy to file operations, blocking the ability to drag and drop files between the user's file system and the corporate file system within the container. In addition, you can log file operations to provide an audit trail of the user's activities. Administrators also can apply a policy to prevent access to the container when copied from one device to another — the container would be accessible only from devices known to the management system.

Streamline the onboarding of new employees by simplifying the process of joining an Active Directory domain. Joining an Active Directory domain allows a user to access corporate resources such as email, file servers and printers. Typically, the user needs to access the corporate network to join the network and then reboot the computer. But some employees might be outside of the corporate network. The Desktop Workspace domain join process is designed to be faster and more transparent for users. Employees can often join the domain remotely and without rebooting.

## Features

**Centralized endpoint management:** Simplify image creation, provisioning and updating. Manage and update one common version for all users with a single base OS image "golden master."

**Comprehensive container security:** Securely manage and deliver the corporate applications and data employees need in the merged business, regardless of which corporate base image is on their system. Plus, keep the enterprise workspace from being moved or edited. Remote revoke and kill policies with an encrypted enterprise workspace protect corporate IP and data if a system is lost or stolen.

**Local execution and simplified access:** Give employees access to corporate resources anywhere, anytime, with excellent response times, even while offline. Streamline user access with Active Directory and two-factor RSA® SecurID® authentication.

**Anti-virus, backup and recovery:** Built-in AVG® anti-virus scanning consistently monitors key loggers and screen scrapers, and scans the host computer at startup. Silent backups of the virtual file system are performed to the management servers. Windows image rejuvenation allows users to recover from viruses.

**AES-256 virtual disk encryption:** Help ensure compliance with government regulations and prevent data leaks.

**Minimal bandwidth requirements:** Update Windows images with only the differences delivered instead of a complete image.

## 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. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

The container provides groups within the business a secure, managed environment for applications and data required for operation of the merged business, but not available on their corporate Windows image.

Dell Software
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
If you are located outside North America, you can find local office information on our Web site.


Datasheet-DesktopWorkspacM&E-US-VG-24363