Desktop Workspace for BYOD

Support end user productivity while maintaining centralized control and security

More and more organizations are embracing bring-your-own-device (BYOD) policies for savings, productivity, or employee satisfaction. Road warriors, remote office and home-based employees, contractors, and even senior executives have personal PC and Macs that need to be managed and secured. But the challenge is providing secure access to corporate networks while managing enterprise data and complexity. This has to be done without crippling device functionality for the user's personal applications, or making end users feel their privacy and personal data security has been compromised. BYOD users also want to be able to use their personal systems for enterprise use at any time and any place. They expect to be able to use applications whether connected to a network or not. Offline use makes remote desktop or application streaming fall short of user expectations and needs.

Dell™ Desktop Workspace—a component of Dell Enterprise Mobility Management (EMM)—solves today's enterprise computing paradox by supporting both end-users' productivity on the laptop of their choice and your need for centralized control. This solution provides flexible, comprehensive mobile enablement through a secure, managed container with a corporate Windows image for laptops.

Container management for BYO PCs or Macs

Desktop Workspace provides a way to securely manage all enterprise applications and data on PCs and Macs in your IT environment, regardless of who owns them. Desktop Workspace's secure, managed container delivers a corporate Windows® image providing low-friction integration with your IT infrastructure and processes, and prevents the comingling of enterprise

Benefits:

- Allow employees to use their own systems and personal applications while protecting enterprise data from leaks and IP loss with a secure container
- Reduce IT costs and increase employee satisfaction by eliminating corporate-supplied laptops
- Improve productivity allowing employees to access enterprise apps and data at any time, any place, on any network
- Maintain productivity offline and in low bandwidth environments
- Simplify image management, updating, and removal of enterprise applications and data with remote wipe of the enterprise container
- Gain policy-based, secure corporate access regardless of laptop OS or network

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

Desktop Workspace delivers a secure corporate Windows image for laptops, with low-friction integration with your IT infrastructure and process.

applications and data with the employee's own applications and data. This solution helps protect critical IP, eliminate IP and data leakage, secure corporate access, protect your network from malware infections or unauthorized intrusions, and simplify endpoint management of corporate applications and data for personally owned devices. Should an employee's PC or Mac get stolen or the employee exits the business, all enterprise applications and data can be remotely wiped from the employee's PC or Mac. It's a dynamic solution that helps IT maintain centralized control while distributing trust out to employee systems.

Desktop Workspace provides a container that runs a corporate Windows image, including OS, applications, and data, on a PC or Mac. For employees, the applications delivered in the Windows image may access critical business data such as business operations systems, financial and accounting data, business and product plans, customer service and support systems, email, corporate directory, VPN clients, etc. The container is physically and logically separate from the OS, applications, and data on the employee's host system. You manage the container without affecting an employee's personal applications and data.

Today's challenge is providing secure access to corporate networks while managing enterprise data and complexity.

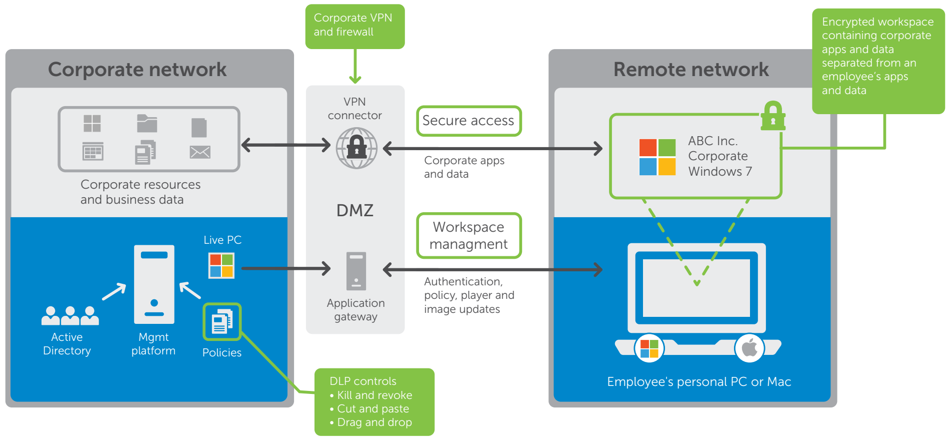
The container solution provides a robust set of policies to manage the container and the Windows image. You can create an image and apply a set of policies at deployment time. Should you need to adjust management policies to be more restrictive or permissive, new policies can be dynamically applied to the user's container.

Two policies that are applied dynamically to protect corporate applications and data within the container are Kill and Revoke. These policies provide critical controls allowing you to immediately secure corporate apps and data should a suspected security breach occur or if a PC is lost or stolen. Revoke is applied to prohibit a user from accessing the corporate image in the container. The image and data still reside on the user's PC or Mac. The user can't access the image and data until reauthorization by the IT administrator. Kill allows the IT administrator to destroy the container and its contents. When employees exit the business or lose a device, Kill can be used to remove all enterprise apps and data from their system.

Desktop Workspace provides policies that prevent loss of corporate data, such as customer information, business plans, financial data, or other IP, being exposed through applications on the employee's PC or Mac. A policy can be applied to prevent copy and paste of data between enterprise applications and personal applications. A policy can be applied to file operations to block drag and drop of files between the user's file system and the corporate file system within the container. Logging of file operations can also be done to provide an audit trail of the user's activities. Additionally, a policy can prevent access to the container when copied from one device to another. The container will only be accessible from devices known to the management system.

Joining an Active Directory domain is a key process for you to provision a new computer system. This allows the user to access corporate resources such as email, file servers, and printers.

The current state of technology requires that the computer needs to be on the corporate network to join the domain, while this tedious process also requires a reboot of the system. BYOD users are frequently outside of corporate networks. The Desktop Workspace domain join process is designed to be faster and transparent to the end user, and does not require a reboot. End-users can often join the domain remotely reducing the complexity of onboarding of remote or home-based employees and contractors.


Corporate VPN and firewall
Corporate network
Corporate resources and business data
Live PC
Active Directory
Mgmt platform
Policies
VPN connector
DMZ
Application gateway
Secure access
Corporate apps and data
Workspace managment
Authentication, policy, player and image updates
DLP controls
• Kill and revoke
• Cut and paste
• Drag and drop
Remote network
Encrypted workspace containing corporate apps and data separated from an employee's apps and data
ABC Inc. Corporate Windows 7
Employee's personal PC or Mac

IT manages a secure container providing a corporate Windows image with enterprise tools, data, and applications on the employee's PC or Mac connected to the enterprise via a remote network

Features

Centralized endpoint management—simplify image creating, provisioning and updating. Manage and update one common version for all users with a single base operating system image "golden master."

Comprehensive container security—separate business and personal applications and data, plus keep the enterprise workspace from being moved or edited. Remote revoke or kill with an encrypted enterprise workspace.

Local execution and simplified access—give employees access to corporate resources anywhere, anytime, with excellent response times, even while offline. Streamline user access with AD and two-factor RSA® SecurID® authentication.

Anti-virus, backup and recovery—built-in AVG anti-virus scanning provides consistent monitoring of key loggers and screen scrapers, plus host computer start-up scanning. 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—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.

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-DesktopWorkspace4BYOD-US-SW-24239