



DELLTechnologies

How Virtual Desktop Infrastructure Enables Digital Transformation



vmware

Digital transformation, the process of applying innovative digital strategies to improve operations and create new services, imposes a variety of challenges on organizations. Accordingly, the IT playbook for adapting to these changes continues to evolve. Dynamic allocation of IT resources, emerging security concerns and an increasingly remote workforce are just some of the factors organizations have to address while remaining competitive.

Virtual desktop infrastructure (VDI) is a foundational technology that many organizations leverage as part of their digital transformation strategy.

This guide covers:

- Common characteristics of adaptive organizations. 3
- Challenges managing desktop infrastructure. 4
- Key aspects and benefits of VDI. 5
- Evaluating VDI options. 6
- Next steps. 8



Virtual desktop infrastructure (VDI) is a foundational technology that many organizations leverage as part of their digital transformation strategy.

Common characteristics of adaptive organizations.

Organizations that are thriving when it comes to digital transformation share key characteristics.

They are agile.

These organizations change their focus, processes and resource allocation according to changes in the market and external environment. Software engineers are an example of specialty workers who have developed agile practices that are based on constant feedback from end users. Because developers receive continual feedback on their work, they can correct mistakes quickly and take advantage of unanticipated opportunities presented by end-user feedback.

They focus operations on value-adding processes.

For instance, operational overhead and basic maintenance do not necessarily add value, though this work is required. Agile organizations minimize these necessary tasks. One way to reduce operational overhead is to leverage hyperconverged technologies. This kind of infrastructure combines multiple data center technologies—such as servers, storage and networking—into single units that employ virtualization to allocate resources on an as-needed basis.

They leverage hybrid clouds to reduce operational overhead.

Organizations that can identify workloads that run optimally in the cloud can take advantage of on-demand compute and storage resources. Not all workloads, however, are suitable for public cloud environments. For example, workloads that require low latency access to large volumes of data stored in on-premises systems are better supported on-premises. For workloads that cannot be moved to public clouds, enterprises can leverage the same technologies that have made public clouds so successful, including virtualization. The combination of public cloud and on-premises infrastructure, commonly referred to as hybrid cloud, enables more strategic workload placement.

They enable individual contributors in the organization to leverage technology.

The ability to work remotely is an important one. Organizations radically expand their pool of potential employees and contractors when they can tap into labor markets across the country or internationally. Analysts and specialists are increasingly making use of high-performance desktop computing to leverage data science, machine learning and other compute-intensive practices.

They are cognizant of implementing best practices for information security.

Wherever a desktop is deployed, it is up to date and patched while also appropriately configured to secure resources; furthermore, it enables workers to access the resources and tools they need to do their jobs.

Wherever a desktop is deployed, it is up to date and patched while also appropriately configured to secure resources; furthermore, it enables workers to access the resources and tools they need to do their jobs.

Challenges managing desktop infrastructure.

Managing desktop infrastructure requires balancing several key factors, such as ensuring users have the desktop resources they need, making the environment secure and accessible, and controlling costs.

In the past, these factors were easier to balance due to fewer infrastructure options and demands; a small number of standard desktop configurations would satisfy most needs. Although some users required remote access, the typical user was working from an on-site location with access to a locally managed network. Security was, of course, a concern, but there were well-established and understood practices for dealing with security threats. Anti-malware, basic access controls, firewalls and other perimeter security measures were widely used and addressed most desktop security concerns.

The characteristics that defined desktop infrastructure environments in the recent past, however, have since changed rapidly:

Varying demands for desktop resources.

Demands for desktop resources are now more dynamic due to employees changing roles frequently, contractors and consultants joining and leaving organizations regularly, and users finding the need for short-term access to additional resources due to large workloads. This dynamic environment makes capacity planning and resource allocation increasingly difficult. Today's desktop infrastructure environment requires the ability to scale up and down according to demand.

Controlling costs.

Another requirement is the need to control costs. Fixed desktop infrastructure requires capital investment that imposes limitations on how that investment is used. For example, purchasing 1,000 physical desktops requires physical distribution, setup and maintenance. Also, the compute and storage resources in those devices are not easily reallocated to other use cases. This leads to some desktops running with excess resources, while others are constrained by insufficient CPU, memory and storage.

The fundamental problem with physical desktops is that they allocate resources in a long-term, fixed way. Reallocating those resources to where they are needed is slow and expensive. There are many use cases for which physical desktop infrastructure is the optimal choice. For instance, when desktop requirements are consistent for extended periods of time, a physical desktop is a good option. However, it is important to understand the dynamics of workloads and end-user requirements so organizations can make the best investment choice when choosing between physical and virtual desktop infrastructure.

Increased demand for remote access to desktop infrastructure.

Remote work is not new, but it is increasing. Software engineers, for example, could work from virtually anywhere because they had the tools and practices to support remote access to resources. Now people who hold a wide range of roles in organizations are operating remotely. Some organizations were able to readily adapt because they had infrastructure in place to support collaboration, maintain security, and provide multiple ways of accessing compute and storage resources. According to a recent ESG survey, 31% of organizations experience improved support for remote and mobile users with VDI.¹

Securing desktops.

Maintaining secure desktop environments is a significant demand on IT support and information security personnel. Desktops have to be configured securely before they are deployed. Of course, the most secure configuration at one point in time may not be the most secure at a different point in the future. There is a constant need to assess the security status of desktops and ensure they have the latest secure configuration.

Desktops are now one of multiple forms of endpoints, that include mobile devices, tablets and Internet of Things (IoT) devices. These different endpoints are suited to different use cases and support various kinds of business requirements. Collectively, these endpoints make up a substantial set of an organization's IT infrastructure. They require monitoring and maintenance, and that, in turn, means there is a need for tools and services to enable IT personnel to access, assess and adjust those devices.

Physical desktops, while useful and cost-effective in many cases, are not always appropriate for emerging business needs. Organizations need a sustainable infrastructure that is also adaptive.



Key aspects and benefits of VDI.

**VDI is a foundational technology for digital transformation.
Therefore, it is essential to understand its key aspects and benefits.**

Traditional physical desktops typically have high procurement costs and, as noted earlier, they lock in a fixed allocation of compute and storage resources. At best, this is an optimal configuration at a specific time, but it can never be the optimal configuration all the time given how frequently resource demands vary. Software licensing for each individual machine can further drive up the per-unit cost of delivering access to a desktop.

Virtualization and hyperconverged technologies are essential to avoiding these drawbacks of traditional desktops. VDI brings virtualized desktops to an organization using its own infrastructure. This is a cost-effective option when the organization has enough desktop users to warrant the required investment in infrastructure and support staff.

Small organizations with limited IT support may want to adopt virtual desktops, but can lack the resources to procure and maintain the necessary infrastructure. In those cases, a cloud-based desktop as a service (DaaS) may be a better option. With DaaS, users can take advantage of public cloud resources and desktop virtualization provided by a third party.

The key benefits of VDI include streamlined security and compliance operations with respect to desktop infrastructure. Because desktops are centrally managed, it's easier to apply security patches and deploy secured desktops. This capability removes additional legwork for the IT staff, who won't need to push patches to individual devices, ensure they install correctly and address errors in the patching operations.

Dell Technologies brings VDI to a broad spectrum of use cases.

To stay flexible and resilient in times of uncertain demand, secure remote management should remain top of mind as a business requirement. Dell Technologies end-to-end VDI solutions consist of products and services designed to enable organizations to reap the full benefits of desktop virtualization and personal access to the cloud for a broad spectrum of use cases.

For customers that are looking for a turnkey solution, Dell Technologies offers a comprehensive Managed VDI Service that can provide day-to-day, hands-on management of the VDI environment. Desktop virtualization services from Dell Technologies can help organizations identify ideal use cases for VDI, and provide qualitative and quantitative data to support those use cases.

Organizations can benefit from working with a trusted partner while implementing digital transformation initiatives. With the integrated desktop virtualization platform from VMware, Dell Technologies offers organizations the greatest breadth of choice in how their people access cloud-based services that meet today's needs, as well as the full range of possible future requirements.

Evaluating VDI options.

If an organization is considering VDI, there are several features to evaluate.

Assess the capabilities of virtualization software.

This software is a key determinant of VDI performance and, therefore, return on investment. For example, [VMware Horizon](#) simplifies the management and delivery of virtual desktops and apps on-premises, in the cloud or in a hybrid or multi-cloud configuration through a single platform to end users. By leveraging complete workspace environment management and optimized for the software-defined data center, Horizon helps IT control, manage and protect all of the Windows resources end users want, at the speed they expect, with the efficiency business demands.

Dell Technologies cloud-based client virtualization.

Organizations that do not have data centers and the staff to support on-premises VDI can instead take advantage of Dell Technologies cloud-based virtualization services. This offering is especially useful for organizations that want to enable their employees to work quickly while also benefiting from the desktop virtualization environment.

The necessary hyperconverged technology is housed off-premises and all the expense of the compute side is a managed service from Dell Technologies or its partners. The only responsibility of the customer is to connect an endpoint to the network. If an organization is evaluating public cloud as its only option, Dell Technologies can help deploy that same model while maintaining control, flexibility and security.

Harden virtualization software to help maintain security and organizational compliance.

The security advantages of VDI are well understood. Nearly 8 in 10 organizations believe VDI or DaaS is more secure than traditional desktop provisioning, according to ESG.¹ Much of the security optimizations available in VMware are built on features of Intel® architecture, including Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and Intel® Trusted Execution Technology (Intel® TXT). Intel® AES-NI provides encryption acceleration, while Intel® TXT moves the root of trust out of software and into hardware.

In addition, there are multiple other security advantages, including NSX, which enables improved VDI scaling and security, as well as AppDefense—a part of vSphere—that hardens the hypervisor and reduces the attack surface. Furthermore, Carbon Black provides additional automated detection capabilities to the servers/DC running the VDI instances.

Review the networking capabilities of the platform.

Ideally, key networking functionality is delivered with a combination of flexible, easy-to-manage software and performant hardware. For example, [Dell EMC SD-WAN](#) combines Dell Technologies network appliances with VMware SD-WAN software to provide advanced adaptive networking features such as Dynamic Multi-Path Optimization that reduce costs while improving application performance. Also, consider the value of network optimizations provided by the joint development of VMware and Intel®, including hardware optimization and network virtualization designed for scale and resiliency.

About Intel® Optane persistent memory modules.

[Intel® Optane PMem](#) is a new non-volatile memory technology that can store large amounts of frequently read data for memory-fast access while also offering data persistence, which means that the data remains after it's read or written.

Plan to support a variety of endpoints and consumption levels.

VDI should be able to support all of the endpoints currently deployed. It should also be designed with enough adaptability to accommodate other types of endpoints that may be employed in the future. There is an increasingly diverse array of client endpoints, so it's essential that VDI is designed for client devices that handle Unified Communications and other content optimizations.

Develop a strategy to support flexible consumption.

One of the most important features to understand is scalability and the ability to support flexible consumption of resources. [Dell Technologies On Demand](#) allows organizations to pay for what they use and pay as they grow, rather than commit to a fixed set of infrastructure investments for extended periods of time.



Scalability applies to two dimensions: the number of users and the resources allocated to a user.

Large organizations will need to support a large number of users, so it's important to have infrastructure that can meet that workload. With Dell EMC's cost-effective [VDI bundles](#) coupled with the [right client for VDI](#), managed services and flexible deployments can easily add more infrastructure as demand grows. Users will require different levels of compute and storage resources over time. VDI management services should allow users to quickly obtain access to the resources they need, keep them as long as needed and deallocate them when they are no longer needed.

Streamline data management solutions.

[Dell EMC VxRail](#) appliances leverage a wide range of software and tools, including resources co-developed by Dell EMC and VMware for an enhanced VDI solution. The VMware hyperconverged software is vSphere-ready and based on vSAN Software-Defined Storage (SDS). Dell Technologies deployment and support tools integrate the software management within VxRail Manager. Data protection and replication are included and can support either hybrid or all-flash storage configurations.

According to ESG, "VxRail with Intel® Optane PMem enables organizations to consolidate more applications, even those with high-performance needs, to gain the deployment and management efficiency benefits that HCI offers. It also expands the range of VxRail-applicable workloads at the core, edge, and cloud."²

Next steps.

VDI is a technology that enables organizations to deliver new services and optimize the delivery of existing applications by making compute and storage resources available to those who need it when they need it. This solution is particularly cost-effective when coupled with [pay-as-you-go, cloud-based services](#).

Dell Technologies brings an array of optimizations and enhanced technologies that are possible only through close collaboration with partners such as Intel® and VMware. Together, we have created a VDI platform that enables adaptive organizations to bring transformative digital services to their users.

[Learn more about VDI benefits with Dell EMC Ready Solutions for VDI.](#)



Sources

¹ ESG Research, Trends in Digital Workspaces, VDI & DaaS, April 2020. Full Report: <https://www.dellemc.com/resources/en-us/asset/analyst-reports/solutions/esg-ebook-digital-workspace-vdi-and-daaS-trends.pdf>

² Based on ESG Technical Validation commissioned by Dell Technologies and Intel®, “Dell EMC VxRail and Intel® Optane Persistent Memory”, July 2020. Actual results will vary. Full report: <https://www.dellemc.com/en-us/collaterals/unauth/analyst-reports/products/converged-infrastructure/esg-tech-validation-dell-vxrail-and-intel-optane-pmem.pdf>