Security Benefits of DaaS

May 23, 2018 / Erika von Hoyer, MBA

You may be surprised to hear that desktop security is arguably the biggest and most important benefit of implementing Desktop as a Service (DaaS) for your organization. Physical desktop computers with locally installed operating systems and applications are expensive, maintenance-intensive, pose security risks, and they can't effectively support the rapidly changing business landscape. Modern business and IT trends such as the ever-growing virtual workforce, ubiquity of mobile devices, and demand for bring your own device (BYOD) support, groundswell of Windows 10 migrations, and tighter IT budgets, all point to the need to reevaluate business desktop strategies.

By virtualizing desktops and applications and moving to the cloud, organizations can realize all the benefits of virtualization and the cloud — centralized and simplified management and orchestration, greater business agility, improved security and compliance, and reduced IT capital expenditures (CAPEX) and total cost of ownership (TCO) — across their entire IT infrastructure portfolio, from servers, storage, and networking to desktops and applications.

Desktop as a Service (DaaS) is the delivery of a virtual desktop offered as a hosted service by a service provider. DaaS has the potential to radically change the way desktops are purchased and managed. However, as is typical with disruptive technologies, there is a good deal of confusion about DaaS and continued misinformation regarding cloud security.

Virtual Desktops hosted through a reputable Cloud Service Provider (CSP) can deliver high-performing desktops to users on any device in minutes, easing IT management burdens and reducing the total cost of desktop ownership, by consuming virtual desktops as a cloud-hosted service. While performance and management are valued benefits of DaaS, without a doubt, security is one of the most important benefits of virtualizing desktops.

Here are three ways in which DaaS can increase the security posture of an organization:

1. Enhance security and compliance.

Security breaches often take place at the edge of the network. So, DaaS is an attractive security option because data and applications reside in the cloud, rather than on vulnerable end-user devices. DaaS also helps alleviate another challenge associated with BYOD by enabling a consistent set of security controls across mobile devices, regardless of operating system or hardware.

Finally, cloud service providers typically have far greater security resources available to them than in-house IT staff. Thus, DaaS customers can leverage the security expertise of their service providers to improve their security and compliance posture.

2. Maintain control and privacy.

A common misconception about cloud computing, in general, is that organizations give up some of their control and privacy in the cloud. But ironically, the cloud can actually enhance an organization's ability to control its computing environment and the privacy of sensitive data, particularly with respect to DaaS.

Organizations can create standard desktop images in the cloud, and deliver a desktop environment to their users on any device running any operating system. Virtualized desktops can be persistent (enabling users to save custom settings) or non-persistent (no changes are saved after the user logs out) based on the organization's and the individual user's needs.

Data privacy is ensured in DaaS because no data is ever downloaded, stored, or processed on the local device — it's only displayed on the device. The organization can store data in an on-premises data center or in a public cloud, and apply any appropriate security safeguards, such as encryption, anti-malware protection, data loss prevention, and access permissions, as needed.

3. Eliminate "shadow IT".

Shadow IT cultures often emerge when IT organizations are inflexible or unresponsive to end-user needs. This lack of flexibility and responsiveness, perceived or real, may be the result of the following:

- Budgetary constraints that make it infeasible for users to always get the "latest and greatest" desktop or laptop PC, mobile device, or apps

- Security and compliance restrictions that require a "locked-down" configuration that does not allow users to customize their desktops or install their own apps

- Limited IT staff resources that are constantly absorbed in daily administration tasks or engaged in reactive "firefighting"

DaaS can help organizations eliminate many of the causes of a shadow IT culture by enabling BYOD policies so that end users can use their own personal devices to get work done, without compromising on standards and security. DaaS also frees up IT staff by empowering end users with self-service tools, centralizing and simplifying desktop management, and accelerating mean time to resolution (MTTR) of desktop issues. For example, many common issues simply require the user to reboot his/her virtual desktop to get a new image.

Unfortunately, few IT organizations have the luxury of bigger and more specialized IT staff today than they did even a few years ago. So, leveraging expertise across the cloud is an important "force multiplier" for organizations planning to deploy desktop and/or application virtualization. DaaS doesn't require the same level of expertise and experience that VDI deployments require, which cuts down on deployment and support requirements for in-house staff. Time, money, and talent otherwise spent on transitions to virtual desktops can instead be allocated to transformative applications and other sources of IT-enabled innovation.

Read more about Desktop as a Service and the related solutions.