Workspot.

PC or VDI or Secure Browser?

Considerations for secure end user computing

Businesses of all sizes are currently confronted with the need to secure their end user computing (EUC) environments for their distributed workforces. Organizations are looking at three basic options going forward:

a. Continue to use PCs with all apps and data resident on the physical device
b. Use VDI, where apps and data reside in a secure data center or cloud, and the endpoint device merely serves as the end-user access interface
c. Use a secure browser on an endpoint device to access all apps and data in the cloud

There are advantages and potential shortcomings with each approach, so let's discuss these alternatives.

Windows PC is the #1 attack vector

Windows PCs are the #1 target for malware, including ransomware. By some estimates, Windows PCs are the targets of between 80-95% of malware attacks.

Virtual Desktop Infrastructure (VDI) is more secure than PCs

VDI is more secure than PCs because hosting business data on centralized servers creates multi-layered security, much more than storing it on local endpoints, each of which are potential malware targets. The logic is quite simple – do you want your organization's data located in one or two physical places or in thousands?

Aren't all apps Web? All we need is a secure browser

As more applications are web-based, the question is whether a secure browser is sufficient, especially when it comes to accessing a range of apps, management, and control.

PC vs. VDI vs. Secure Browser?

The question comes down to this: based on multiple factors of end-user productivity, IT management, security, performance, and cost, which of the three choices fit best for secure end user computing – PC, VDI, or secure browser?

Legacy VDI: Complex, Expensive, and Prone to Poor Performance

Many customers call VDI "Very Difficult Infrastructure". This reputation was borne from all the issues created by VDI – boot storms, the noisy neighbor problem, performance of storage, volume of storage, de-duplication, pod architecture for every 2000 or so users, etc. Legacy VDI solutions were designed to be deployed by a single customer in a single data center. Each customer was responsible for operating their own deployment – scaling, upgrading, trouble-shooting, etc. In addition to being complex for IT to operate, end-users oftentimes become disappointed with their VDI solutions. They have complaints about problems connecting to their virtual desktop and having a poor user experience when they can connect.

Cloud-Native VDI Simplifies VDI

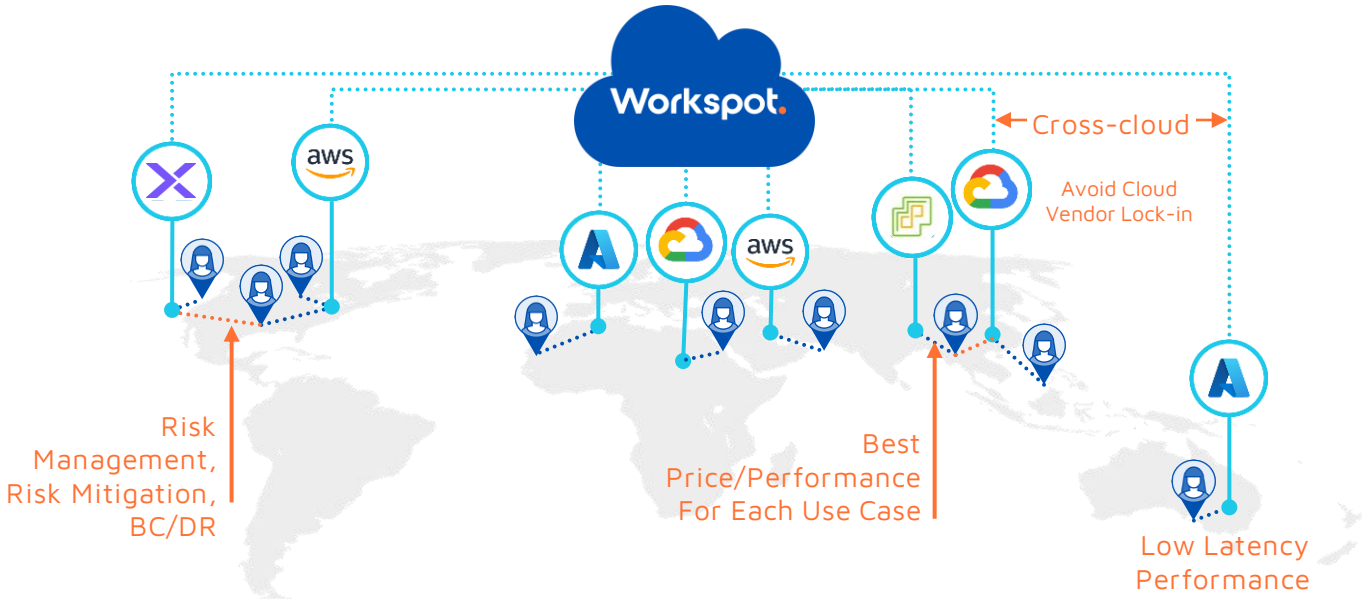
As mentioned above, Legacy VDI solutions burden organizations with time-consuming and error-prone tasks per deployment, management, and operations, which also increases ongoing costs. In an attempt to help alleviate these drawbacks, many of the legacy VDI solutions were extended to the cloud where the vendor took responsibility for operating the deployment, but these solutions had limitations because of their single data center origins – minimum number of users for customers, minimum number of users per region, separate interfaces for each cloud, different architectures for hybrid vs. cloud, etc.

In the last five years, a few cloud-native VDI solutions, like Microsoft AVD, Microsoft Windows 365, Amazon WorkSpaces, and Workspot, have emerged. These solutions were designed from the ground up as cloud services to be consumed by multiple customers. The VDI service provider is responsible for operating the service – scaling, upgrading, troubleshooting, etc. A cloud-native solution for VDI can deliver tremendous performance, cost, availability, operational, and even security advantages to customers.

By eliminating the need to install, upgrade, and patch a myriad of interconnected and co-dependent components, cloud-native VDI dramatically simplifies VDI.

Cloud-Native VDI Can Deliver PC-like Performance

Whereas mono-cloud solutions like Microsoft Windows 365, or Microsoft AVD, or Amazon WorkSpaces can leverage only a subset of their own data centers, a hybrid/multi-cloud solution like Workspot can leverage any cloud and any on-premises data center. With Workspot, virtual desktops and applications can be deployed in a region closest to the end user, thereby reducing latency to <50ms, and delivering local PC-like performance for end-users, almost anywhere.



Secure Browser

A secure browser is a good tool if the use case is for an end-user to access only web applications. A secure browser can offer many of the following security and control capabilities:

- Access to approved websites
- Prevent downloading of plugins
- Prevent downloading of files
- Control copy-paste
- SIEM integration of browser events

But a secure browser has limitations. Google Chromebook is a great case study to understand the impact of secure browsers. Even though Chromebooks are significantly more secure than a Windows PC, they remain at 5% of market share more than a decade after launch.

There are multiple reasons:

- If the use case needs a single Windows application, then a secure browser isn't the right choice. You need a VDI solution or a Windows PC.
- If the use case involves more than 3-7 applications, then a change in user behavior is needed for them to learn how to use a browser to switch between applications, download data, etc. End users have been trained on these workflows on Windows, Mac, iOS and Android.
- You need a network connection to access the applications.

Solution Capabilities Comparison Matrix

We have captured the relative strengths and weaknesses of each solution in the following table. A secure browser is the most secure and inexpensive option, but it can be applied only to use cases that are web applications. Cloud-Native VDI can deliver great security and user experience at moderate cost. However, the solution needs network connectivity. PCs are the most versatile solution, except for compliance use cases.

	Secure Browser	PC	Cloud-Native VDI	Legacy VDI
Limitations	Network Connectivity Only Web Apps	Data Compliance	Network Connectivity	Network Connectivity
TCO per user per month	$10	$50	$50	$100
Security	Good	Poor	Good	Good
User Experience	Good	Good	Good	Poor

User Personas and Use Cases

Focus on the requirements and user personas to drive the choice of solution.

	Managed PC			Zero Trust Endpoint		
	PC	PC + VDI	PC + Secure Browser	VDI	VDI + Secure Browser	Secure Browser
	Windows OS Desktop	Windows OS + Windows Apps + Web Apps	Web Apps Only	Windows OS Desktop	Windows Apps + Web Apps	Web Apps Only
Contractors				✓	✓	✓
Call Centers		✓		✓	✓	✓
3D CAD Engineers	✓	✓	✓	✓		
Developers	✓	✓	✓	✓		
Remote Employees	✓	✓	✓	✓		
Compliance		✓	✓	✓	✓	✓
Knowledge Workers	✓	✓	✓	✓		
Road Warriors	✓	✓	✓			
Frontline Employees					✓	✓

The Verdict

It's clear from this discussion that the answer on which end user computing solution to choose is, "it depends", understanding that the various approaches can overlap each other in terms of their respective plus-factors.

Each organization needs to take a thorough "inventory" of all their end-users needs along with the primary goals of the IT organization and the company. In many cases, an organization will embrace more than one of the approaches above or even have all three, especially when transitioning from legacy VDI to cloud-native VDI, for example. It's important to understand that the use cases table above highlights the *primary* use cases that are ideally served by each approach, and that they are not exclusive.

See it in action – Schedule a Demo!

The Workspot digital workplace platform provides unified, secure access to all virtual desktops (VDI), virtual apps, and secure browsers. It offers a single client for end users on any device from any location and a unified management console for both on-premises and cloud environments. With built-in observability of all end-user activities, Workspot ensures outstanding digital experiences (DEX). As a secure and cost-effective SaaS digital workplace platform, Workspot is the optimal EUC solution for modern enterprises.