CAMEYO

eBOOK

From Application Virtualization to Virtual App Delivery (VAD)

Securing & Simplifying Access to Apps on Any Device

A growing number of IT departments are starting to recognize that one-size-fits-all virtualization strategies are holding back their users. For a long time desktop virtualization technologies like Virtual Desktop Infrastructure (VDI) and Desktop-as-a-Service (DaaS) from the likes of Citrix, VMware, and Microsoft have been the default approach for many organizations. But in the past two years it's become clear that virtual desktops are not necessary for every end-user and every use case—especially at a time when work-from-home policies and remote work environments demand more flexibility.

Obviously, there are many technologies on the market. But to make things even more challenging, It can be difficult to differentiate between the various terms and technologies used to describe these various technologies. For instance, what's the difference between Virtual Desktop Infrastructure (VDI), Desktop-as-a-Service (DaaS), and Virtual App Delivery? And what role does each of these technologies play in the overall "Digital Workspaces" category? Also – whatever happened to "Application Virtualization" and "App Streaming", and how do those differ from Virtual App Delivery?

Let's take a closer look at these different technologies to compare and contrast their capabilities, and to help identify which technologies in the Digital Workspace stack are the best fit for your organization's specific needs.

In This Guide

Virtual Desktop Infrastructure (VDI), Desktop-as-a-Service (DaaS), and Virtual App Delivery

Many organizations today are using **Virtual Desktop Infrastructure (VDI)** to deliver business-critical resources to remote workers. It is a popular option. However, it can be both challenging and costly to implement. First of all, what is VDI? In general, it refers to solutions that pool together desktop resources on a centralized server and deliver these to end-users. The end-user is then able to access the full desktop and run applications, and access data. VDI is a pre-cloud technology that businesses generally deploy in on-premises environments.

Citrix Workspaces and VMware Horizon are two of the major players in this space, and many organizations choose solutions from these solutions to deliver VDI in their environment. What are the challenges with VDI? VDI is notoriously expensive and resource-hungry. It usually requires a dedicated set of servers, storage, and network infrastructure to deliver virtual desktops to end-users in a performant way.

To go along with the dedicated servers, storage, and network infrastructure, organizations generally have to hire at least one or two engineers who specialize in VDI to manage, configure, and troubleshoot the environment daily. The ongoing costs of both dedicated hardware and a team of professionals to manage and maintain the VDI environment can add up.

There have been efforts to overcome challenges and costs with managing an on-premises VDI environment, such as **Desktop-as-a-Service (DaaS)**. With DaaS, the hope is to abstract some of the complexity by shifting the underlying infrastructure to cloud environments so organizations can operate the VDI offering as a service and not deal with the infrastructure side of things. However, DaaS still requires the cloud expertise to deliver the solution, and the underlying complexity is still there. It can also lead to costly spending on cloud services.

Which leads to another key technology in the Digital Workspace stack – **Virtual App Delivery (VAD)**. When businesses start to look at what is most important to enable anytime, anywhere productivity for remote end-users, it is generally the applications. When connecting to VDI or DaaS environments, many remote workers are simply accessing business-critical applications and not interacting with the desktop environment for other reasons. In those cases, VDI/DaaS are overkill, and both the IT environment and the user experience can be simplified with Virtual App Delivery. But it's important to note that it's usually not always an either/or proposition – in many organizations IT can utilize VDI/DaaS for the users who truly need a full virtual desktop, and then utilize Virtual App Delivery for everyone else.

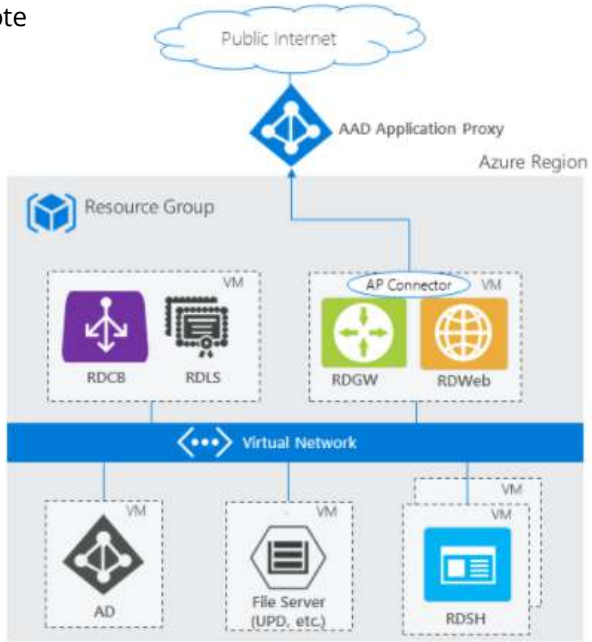
But Wait – What About Application Virtualization & App Streaming?

The concept that not every user needs a desktop is not new. Application virtualization first emerged many years ago to address this issue, and to provide a simpler way to just provide apps instead of full virtual desktops. App virtualization has been around for a while on many different platforms, such as Microsoft Remote Desktop Services, with the aim of providing a more efficient approach to delivering applications to the end-user without the full desktop. App virtualization provides a more efficient footprint and is capable of greater user density per server resource. However, the App Virtualization approach generally requires the same infrastructure configuration whether full desktops are delivered or not. Below is Microsoft's architecture overview of Remote Desktop Services, housed in Azure. There are many moving parts and components, including Remote Desktop Gateway, Remote Desktop Web Services, Remote Desktop Session Host, Active Directory, File services, etc.

Application streaming works a bit like conventional video streaming whereby a user is able to access an application stored on a remote server on demand. When the user initiates that request by, say, clicking an icon in their operating system's GUI, only then does the app start to download to the endpoint.

By copying essential code at the outset rather than the entire software application, the user can start working with the software program almost immediately—just like you can start watching a streaming video with only a few megabytes in the buffer. Meanwhile the rest of the application data will continue downloading in the background.

But even though we're talking about application streaming, this approach tends to rely on the same platforms that are used for desktop virtualization. Streaming applications don't simply run on any operating system. They require a dedicated virtualization or viewing client. This means that all the same infrastructure, costs and management that are bound up in virtual desktops are also part and parcel of application streaming.



Virtual App Delivery vs. App Virtualization & App Streaming

So, what's the difference between Application Virtualization/App Streaming and Virtual App Delivery? Think of **Virtual App Delivery** as the next-generation of App Virtualization/App Streaming. Virtual App Delivery is the cloud-native approach designed to address the challenges and hurdles of legacy App Virtualization by automating away all of the complexity seen in the diagram above. A modern Virtual App Delivery platform should display the following three key characteristics:

- Simplicity
- Seamless Connectivity
- Intrinsic Security

Simplicity

App virtualization products require the same infrastructure needed for full virtual desktops. It results in unnecessary complexity from an architectural perspective and requires numerous components to ensure the solution is reachable, highly-available, and secure. The term **Virtual App Delivery** emphasizes the importance of the *delivery* of the application to the end-user. The delivery must be seamless and straightforward, as we will see.

Seamless Connectivity

With the tremendous transition to remote work in 2020 and continuing this year, employees continue to work from many different locations. They use many types of devices to access business-critical applications and data. However, there is generally one type of access that all devices, both traditional and mobile, have in common – a browser. Modern Virtual App Delivery solutions must provide seamless connectivity to all of the applications people need to be productive from anywhere and on any device through an HTML5 browser. This eliminates the requirement for a "fat" client and allows fully encrypted sessions through SSL encryption.

Intrinsic Security

Cybersecurity has never been more critical than it is today. With record numbers of cyberattacks and new threat vectors popping up each day, today's digital workspaces using Virtual App Delivery must deliver security intrinsically as part of the solution. With traditional remote access and app virtualization solutions, security is an afterthought or a "bolt-on" component. This approach is no longer sufficient, so it's important to ensure that any Virtual App Delivery solution you're evaluating has security built in at the very foundation.

Cameyo - Secure Virtual App Delivery (VAD)

There's no question that today's employees need to access business applications from anywhere and on any device. Cameyo's Virtual App Delivery platform provides the foundation for a robust Digital Workspace that delivers virtual apps to remote workers with simplicity, seamless connectivity, and security.

Simplicity

Unlike legacy application virtualization solutions, Cameyo is purpose-built and engineered for modern Virtual App Delivery. It means there are no unnecessary architectural components in the way of servers, storage, or networking required. It eliminates the cost and management complexity involved in managing VDI and DaaS and other legacy application virtualization solutions.

Customers who choose the on-premises solution can use a single Cameyo execution server on-premises (two recommended). For those who want to use Cameyo as a Cloud SaaS offering, Cameyo offers a fully-managed customer cloud environment for hosting applications.

The Cameyo Virtual App Delivery solution architecture is straightforward:

- The end-user requests to initiate an application by invoking a "play" action URL from the Portal in the form of: https://online.cameyo.com/apps/1234..../play This can also be invoked through a Cameyo API.
- Portal checks the user's authentication for this application. If authentication is required but missing, the portal authenticates the user either through login credentials or the configured SSO provider. SSO can be any OIDC-compliant provider, including Azure AD, Google, Okta, Ping, etc.
- The Cameyo cloud portal communicates with Cameyo "execution" Servers, which deliver applications to end-users.
- The Cameyo execution server responds to the portal with the connection details. The portal translates them to the client:
  - HTML5 client: user's browser is forwarded directly to the server's HTTP/S address with a given token. The execution server then verifies that token against the portal.
  - Native Windows / Android RDP clients: connection is made directly through RDP, using one-time credentials generated on-the-fly and transmitted to the client.
- The session runs according to Cameyo's policy settings such as maximum time / idle time, cloud storage virtualization/synchronization, shell lockdown, toolbar options, file transfer permissions, etc.
- Upon the session's end, the user profile is cleaned up. If Cameyo is configured to "Temporary User Profiles," the entire user profile data is wiped out of the server. If SessionSync is enabled, this is done after synchronizing the user's data back to the central / cloud storage.

Seamless Connectivity
Cameyo provides seamless connectivity to all Windows and internal web applications from any device. Customers' end-users only have to have access to a browser to run the full desktop of any application from their browser with Cameyo. This means end users have nothing new to learn – they simply access the applications they'e always utilized, just via a browser tab instead of an installed app.

Intrinsic Security
Cameyo is built with a zero-trust security model from the ground up. Cameyo never exposes the execution server to the public-facing Internet. Using its unique RDP and HTTP/S Port Shield technology, only authenticated sessions can communicate with RDP and HTTP/S ports on Cameyo servers. Once authenticated, end-users only have access to the sanctioned applications and never to the core system components. Additionally, when a user logs off, Cameyo Port Shield removes the end-users' IP address from accessing the Cameyo server at a network layer.

The intrinsic security provided by Cameyo allows organizations to provide access to business-critical applications on any device, even non-IT managed personal devices, without the danger of data leakage, malware, or other compromising behaviors.

Which Strategy is Right for You?

Although application virtualization or application streaming may suit some use cases, Virtual Application Delivery (VAD) enjoys several clear advantages in most scenarios. These are most apparent in what VAD doesn't require.

- VAD is an enterprise-grade virtualization technology that doesn't depend on cumbersome virtual desktop infrastructure. It's more versatile, more cost-effective and easier to deploy at scale.
- With VAD, end-users don't have to download and run a dedicated virtualization client. Cameyo's VAD solution in particular gives users direct, secure access to all of their business-critical apps on any device with an HTML5 browser.
- The VAD user experience is superior. Users don't have to jump through hoops like logging into a virtual desktop environment. Yet they still enjoy real-time access to the full desktop versions of their business-critical apps.
- Because VAD is easier to manage, IT staff don't have to spend hours wrestling with policy configurations, VPNs, app updates and user privileges. They can easily enable or disable access to apps on a per-user basis.

By the same token, in reducing complexity and cost across multiple areas, VAD realizes all the anticipated benefits of application virtualization. Consider these common use cases:

- Remote & hybrid workers who use secure VAD solutions like Cameyo can stay productive from anywhere without opening themselves up to the risk of ransomware attacks.

- Students can access essential software more easily and from a broader range of devices with VAD.
- Thanks to VAD's versatility, hybrid workplaces can seamlessly bridge the constant transition between in-office and work-from-home schedules.

The best virtualization solution will naturally depend on your individual criteria. But if you're intrigued by the advantages of virtual application delivery, Cameyo represents the best that VAD has to offer. Try out your free trial of Cameyo today and see how easy it is to secure and optimize app delivery for every one of your end users—in as little as five minutes. You also have the option to schedule a demo and have one of our engineers walk you through the features of our Virtual Application Delivery (VAD) platform.