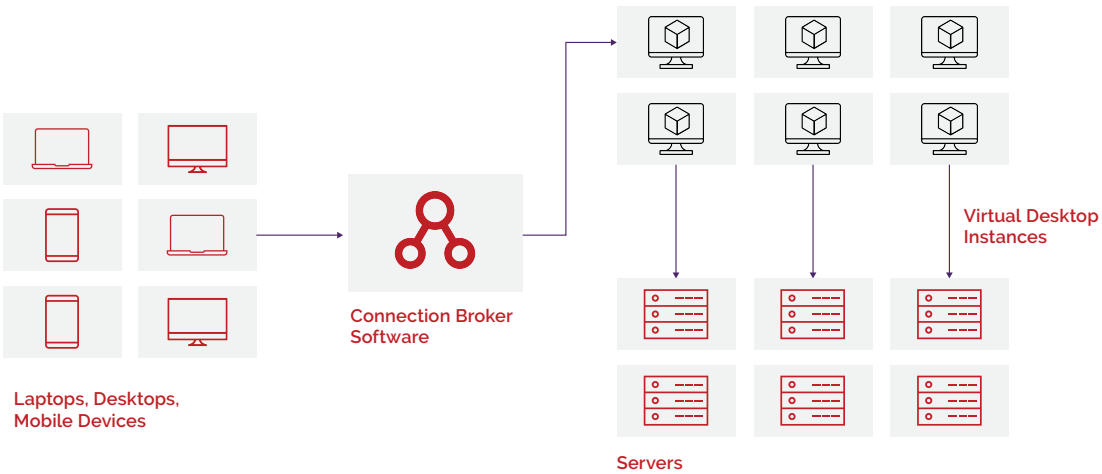
MENLO SECURITY

White Paper

Rethinking VDI in the Modern Enterprise

Virtual desktop technology is well understood, and has been around for more than two decades. While thin client remote desktops go back to the 1990s, the term virtual desktop infrastructure, or VDI, was introduced by VMware in 2006. Products from Citrix and Microsoft quickly followed and adopted this terminology. VDI promised data security and compliance, as well as disaster recovery and business continuity,but while VDI was a compelling solution when it was developed over 20 years ago, a lot has changed in that time. The network perimeter has dissolved, and the advent of the SaaS model has put modern apps in the cloud with many accessible via the browser.

These technologies saw increased use during the pandemic, when enterprises were forced to come up with secure remote access solutions almost overnight. As Computerworld wrote in 2020, "...with companies' entire workforces now connecting to corporate networks from home, sometimes without a company-issued laptop with VPN and all the necessary settings for secure access, VDI is getting a second look."[1]



[1] Pandemic gives VDI a new lease on life, Computerworld, Sept 23, 2020, https://www.computerworld.com/article/3574938/pandemic-gives-vdi-a-new-lease-on-life.html

The infrastructure to support a VDI solution, whether housed in the cloud or on prem, includes clients, a connection broker, virtual machines, and a hypervisor. The client, or end-user device, allows users to access their virtual desktops and applications, which reside on virtual machines.

The connection broker enables the connection between the end-user device and the VMs and hypervisor. The connection broker handles authentication and authorization, along with management of desktop sessions and pools or desktops.

Virtual machines can each have their own OS, apps, and configuration. Final components include the physical servers as well as the hypervisor, which segments the server content onto virtual machines.

VDI was designed to be hosted on-prem in the enterprise data center, although cloud-based versions of the technology have become available. Regardless of where VDI systems are deployed, enterprises must contend with the hardware, software/licenses, and networking infrastructure. And it requires the ongoing attention of increasingly scarce resources—a staff that is cross-trained and skilled in virtualization, network engineering, compute systems, and security. The staff that must install, deploy, manage, and operate every element of the VDI solution represents a significant cost. Staff may also be called upon to handle hardware provisioning, software updates, security upgrades, and day-to-day maintenance.

Virtual machines can each have their own OS, apps, and configuration. Final components include the physical servers as well as the hypervisor, which segments the server content onto virtual machines.

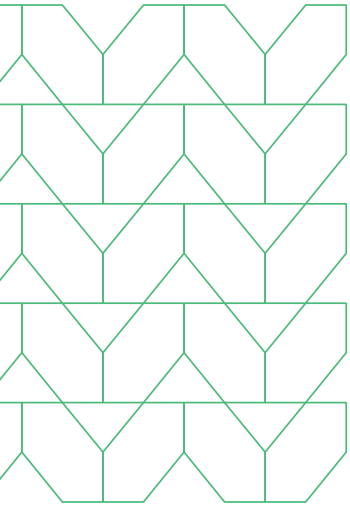
Desktop as a Service (DaaS)

For the end user, the differences between VDI and DaaS are negligible. To security, IT, and infrastructure teams, however, the difference can be enormous. VDI is single tenant by design, while DaaS solutions are managed multi-tenant deployments. But the differences don't stop there. You can think of DaaS as being essentially a VDI managed by a third party. While VDI works for some user profiles, such as those in traditional call centers with a limited set of applications, DaaS merely relieves the enterprise of management, and trades that for pay-as-you-go operating fees. Because hardware and software are provided by the third party, choices are limited. That third party also oversees management, maintenance, backups, and upgrades, security posture and threat response, in addition to compliance and data sovereignty. Many enterprises cannot delegate these responsibilities to a cloud service, so DaaS is not an option in many situations.

Is VDI or DaaS Right Today?

To determine whether your VDI implementation is the right choice today, let's look at what VDI was actually designed to do, including:

- Save money relative to the cost of a dedicated PC for each employee, via thin or BYOD endpoints.
- Enable central monitoring, management, and back up corporate infrastructure
- Provide secure remote access to end users



Costs

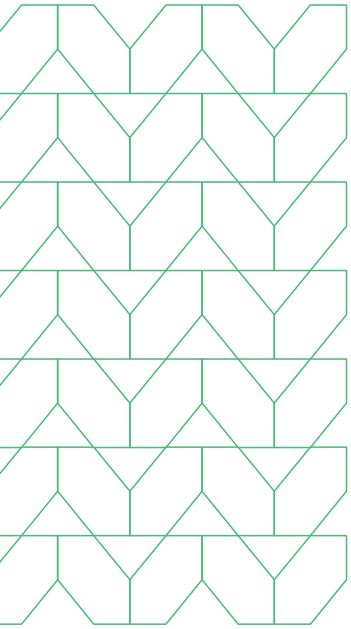
Minimizing cost was one of the most important claims originally touted by VDI developers. The argument for this technology was that VDI would:

- **Reduce admin and support costs** — This benefit depended upon the enterprise having a pool of suitable end users that was large enough to justify the considerable outlay of cash and effort needed to implement VDI in the first place. There are still situations where VDI is justified, but that is likely a much smaller subset of users than it used to be. It is also important to realize that VDI in any form is not a "one-and-done" proposition. Things change in the VDI world as often as in other aspects of networking and computing.

  Another significant and often overlooked factor is that the maintenance of a centralized infrastructure requires a completely different skill set than what is required to manage typical desktops. Any admin that has set up a VDI solution can tell you that they can be temperamental to set up and maintain, with elements that go far beyond the initial infrastructure choice to provide an adequate end-user experience. To make matters worse, some of the most important contributors to end-user satisfaction are elements over which the enterprise has no control. The system requires high-bandwidth, low latency internet connectivity, sufficient compute resources, fast storage, a bulletproof setup, and constant patching.

- **Lower maintenance costs** — Upgrades and maintenance do not go away in a VDI deployment; they are simply moved to other parts of the infrastructure. Maintenance and upgrades, as well as the staff to implement them, can add substantially to the overall price tag. Staying on top of a VDI deployment is particularly vital because, like any centralized model, if any part of the infrastructure runs into an issue it will affect every end user.

- **Reduce hardware costs** — The initial idea was that rather than buying a legion of end-user devices, the enterprise would instead invest in a robust central infrastructure. That reasoning may well have been true when the technology was developed, and may still apply in some areas. Ongoing VDI use has shown, however, that the initial cost of procuring a sufficiently large server to power end-user devices can, in many cases, be more expensive than buying basic devices. The same is true to a lesser extent with cloud-based VDI.



Security

- **Enhance security** — Security has been a driver for VDI adoption. The idea was that by centralizing assets, controlling end-user desktops, and hardening access to backend systems, enterprise assets would be more secure. Another consideration is that there is no end-user device that could be stolen or lost. But the unfortunate fact is that VDI systems can themselves be hacked, which means that threat actors who successfully access centralized assets have a chance of landing a much bigger target. Even without breaching the backend systems, it is possible for data exfiltration and other risks to occur via data transfer to and from endpoints. If any element of the solution were hacked, then every element is effectively hacked.

End Users

The ultimate success or failure of VDI often rests on the distribution of different end-user profiles. If users require particular applications, personalized settings, and above-average compute power, VDI can become much more difficult to manage than a number of enterprise workstations. Another factor is that more technically sophisticated users are more likely to resist a locked-down VDI implementation.

- **Remote workers** — Remote work is one of the biggest reasons why VDI saw such an uptake during the pandemic. Enterprises turned to VDI to enable remote work, and many have not turned back as hybrid/remote work appears to be here to stay. While VDI technically supports remote work, users are often unsatisfied with the experience and the security risks posed by unmanaged browsers on these devices pose a threat. In mobility use cases especially, VDI is notorious for poor performance and can be maddening to use when applications slow down or drop altogether.

- **Flexibility** — A VDI infrastructure was supposed to bring agility to the enterprise, and, in certain situations, historically, it did. For example, when provisioning applications for seasonal workers on a campus or in a fixed logistics environment, the technology lived up to its promise. These benefits can easily be undermined, however, if the overall workforce does not conform to the profile of the workers for whom the solution was implemented. It can be difficult to correctly gauge the number of seats that are really served by VDI, so it is possible to end up with the worst of both worlds, requiring the management of the VDI infrastructure AND managed end-user devices.

Virtualized Desktop Redux

VDI had been around for decades before the pandemic gave it a second life due to the needs of (suddenly) remote workers who needed secure access to applications and resources. DaaS, essentially VDI that is implemented and managed by another party, provides the same benefits at what might look like a lower price point. The impetus for both made sense then, particularly considering that the move to cloud-based apps was not as widespread. But, in the light of today's enterprise priorities and the fact that most cloud-based apps are now accessible via the browser, is a centralized deployment of a virtual desktop really cost effective or even necessary?

Enterprises need a secure solution that can be tailored to their specific industry, and that takes into account emerging compliance and data sovereignty needs. End-to-end visibility is essential, along with the ability to conduct complete forensics. And it is vital to protect enterprise assets from intentional or inadvertent compromise.

A final important consideration is how well these solutions are accepted by the end users that need to work with them. For users best served by a personalized device, the downsides to a centralized solution can include learning a new operating system. Other drawbacks can include the fact that both VDI and DaaS are plagued by poor performance. Applications often run slowly, particularly during peak times, and the virtualized desktops simply do not look or feel like the user's own endpoint.

There's a better way

The solution is now simple—the Secure Cloud Browser from Menlo Security, with Secure Application Access (SAA). Users, including contractors or partners, can work with enterprise-provided desktops or their own BYOD devices. SAA provides access to all popular applications, including those with SSH and RDP protocols, secures enterprise data, and protects applications from infected endpoints. Users are typically much more productive, too, because in addition to their own endpoint, SAA works with the browsers that they already know.

The benefits of Menlo Secure Application Access doesn't stop with the end user, either. Application access can be deployed in minutes, with no need for agents, certificate import, or DNS changes if your application is browser-based. IT and security teams have the benefit of granular controls for data and applications, including read/write, upload/download and copy/paste options. Other benefits include built-in last mile data loss protection, content watermarking, sandboxing and more. SAA enables protection against internet threats, while making apps fully available to authorized users.

The Menlo Secure Cloud Browser offers further protections against today's Highly Evasive Adaptive Threats, including advanced phishing attacks that are often sent from reputable websites. Perimeter and endpoint security will not catch these attacks, but the secure Cloud Browser catches them everyday, including zero hour attempts. If Menlo HEAT Shield is deployed, alerts can be easily investigated before an infestation even starts. And inappropriate end user browser behaviors can now be easily investigated, with Menlo Browsing Forensics. This is a significant reduction in risk for any enterprise.

The Menlo Secure Application Access solution, based on our award-winning Secure Cloud Browser, delivers a complete solution that not only saves money but saves your IT team as well. Centralized monitoring and management deliver secure remote access without the complexity of VDI. End users will enjoy a better experience, and your IT team will be able to react to issues more quickly and easily.

Don't try to solve today's application access issues with yesterday's technologies. Find out if Menlo Secure Cloud Browser and Secure Application Access is right for you.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.