

Brought to you by



Choosing the right client for your virtual desktop solution

By Travis Brown, Senior Product Marketing Manager



Organizations of all sizes have discovered that desktop virtualization can provide employees with increased flexibility and mobility while still safeguarding corporate data. However, streaming the OS, applications, and workloads from a datacenter to enable secure, nearly ubiquitous access is only *part* of the equation. Many IT professionals who have embraced the technology realize their implementation may be overlooking an important element of the most effective VDI architectures, leaving a number of security and productivity enhancements unrealized. Specifically, desktop virtualization solutions are nearly always improved by deploying thin and zero clients that are more secure and cost less to operate than traditional, legacy endpoints.

While many IT departments wonder whether they should repurpose legacy PCs or deploy thin or zero client devices the results are clear — thin or zero clients can maximize user productivity by reducing downtime, avoiding viruses, and malware, and enabling a higher level of control over applications and data. Adding thin clients to a correctly-sized and blue-printed VDI solution reduces operating expense (OpEx) and capital expenses (CapEx) over time.

Thick vs. thin computing

A common misperception about desktop virtualization is that repurposing existing PCs, rather than investing in modern thin clients, is the most economical choice, and it may be from an immediate capital cost perspective. In reality however, the total cost of ownership (TCO) using PCs far exceeds the relatively small capital investment in thin clients, largely due to the cost advantages gained in these operational areas:

Security: Legacy endpoints put data at risk of being copied to other media locally or uploaded to third party online



Adding thin clients to a correctly-sized and blue-printed VDI solution usually reduces operating expense (OpEx) and capital expenses (CapEx) over time.

storage accounts. Avoiding data in flight or moving through the network is a risk that is of particular importance in industries where security and compliance with privacy regulations are a primary concern. While healthcare, government, and financial services are usually the most strictly regulated, retail and education both require special attention to safeguarding personal information. Higher education may be particularly vulnerable, since endpoint security has historically been less of a priority in academic research or with data storage related to education. Thin clients offer a more secure foundation since they lack local drives and their USB ports can be remotely disabled, further reducing the risk of unauthorized data transfers.

Manageability: Because thin and zero clients can be centrally controlled, the need to visit individual endpoints is almost eliminated. Historically, the need to implement OS patches and software updates locally across hundreds or thousands of PCs, led to a significant investment in time and effort. By contrast, thin clients leverage a smaller OS (10kb-20MB) that can be deployed centrally. Deployment can even be automated, where thin client, via an INI file, gets its setting each time a user logs on. A simple change to a single INI can automate updating literally thousands of thin clients. Zero clients need even less management. Instead of a small OS, a zero client's instructions come from firmware. Because the firmware is updated only once or twice a year and because thin and zero clients are managed remotely, IT staffers can be reassigned from "break/fix" work to more strategic projects.

Cost savings: Remote management of endpoints and software requires far fewer resources. Your enterprise can also realize operating savings over time by reducing the number of man-hours required to manage devices. In addition to these OpEx savings, significant CapEx savings can be realized over time because thin and zero clients are less susceptible to mechanical failure. With fewer parts that

can break down, mean time before failure (MTBF) can be as much as much as 30 years. Thin clients are refreshed over a longer interval every 5-7 years versus traditional PCs' 3-5 year refresh rate. With thousands of endpoints in an enterprise, this savings can be significant.

Additional benefits beyond enhanced security, manageability, and cost savings include lower power consumption and a smaller physical footprint in environments where desk space is at a premium. Today's thin and zero clients also offer the ability to use a secure all-in-one device (an attractive Dell monitor with an embedded thin client) that is unobtrusive in customer-facing environments. These benefits also impact the bottom line with savings drawn from:

Less power consumption - Legacy PCs draw significant power to sustain their operations locally. Alternatively, thin client devices require a fraction of the power, supporting green efforts and environmental initiatives. While consumption varies among specific models and workloads, thin clients draw 6-20W of power versus 50-120W for a legacy PC.

Lower cost device - Thin clients have lower I/O requirements given that they only process keyboard and mouse inputs and render virtual desktops and applications streamed from the datacenter. Since the "heavy lifting" of processing workloads is performed in the datacenter thin clients have lower processor and memory requirements — as low as 1GHz processor and 1GB of RAM — and therefore lower cost. Additionally, they do not require incremental hardware upgrades to handle most office-related tasks.

Smaller footprint - Thin clients have a much smaller physical footprint vs. most legacy PCs. Thin clients can be attached under a desk via a VESA mount, affixed to a wall, or VESA-mounted unobtrusively to the back of a monitor. This is an appealing option in environments where desk space is at a premium such as





nurse's stations in healthcare, reception desks in hospitality, checkout counters in retail, information kiosks in malls, or teller stations in banking. Another option is to deploy an all-in-one thin client such as the Wyse 5000 series, an elegant option where minimalist aesthetics are important. These low-impact or minimalist endpoints can help represent your brand and enhance the customer experience.

Thin and zero client use cases

Task worker: primarily text-based workers using one or two applications simultaneously, low multimedia needs; in deployments where total cost of ownership (TCO) is the key driver

Knowledge worker: employees require a high definition user experience, enhanced security, 3D graphics/VOIP/HD Media; and where the user experience is just as important as TCO

Power user: engineers or designers accessing CAD/CAM software, or financial traders running complex mathematical and multimedia applications, or rich media across four or more displays; and in environments where user experience is more important than TCO

Mobile worker: these workers need to access applications and data when no Wi-Fi network or WAN is available — e.g. on airplanes, multimedia over WAN; user experience eclipses TCO savings due to productivity. For users where performance outweighs whatever lower CapEx and OpEx savings may be achievable.

Thin clients vs. zero clients

A zero client differs from a thin client in that it communicates with a VDI environment via a single protocol without a local operating system residing on the endpoint. The decision to deploy zero clients is typically driven by specific user requirements, compliance considerations, or use cases. While both thin and zero clients are specifically designed for environments where small form factors

and solid state computing devices are needed, they differ in processor and memory configuration as well as cost.

Thin clients: Typically use a low-footprint operating system such as a proprietary OS, a Linux distribution or Windows Embedded, a thin version of the full Windows OS. The purpose of the OS is simply to connect the thin client via a connection broker to the users' virtual desktops and to support running hardware and peripherals. This design allows IT to deliver multiple desktop virtualization protocols such as Citrix® HDX, Microsoft RDP/RemoteFX, or PCoIP. Thin clients are ideal for maximum connection broker flexibility. Thin clients have every broker pre-installed while zero clients are typically dedicated to a specific connection broker. The local small footprint OS is simply used to make a virtual desktop connection. The OS is protected on a write-resistant flash drive vs. a traditional PC with an onboard hard drive, with very little risk of OS corruption or downtime.

Zero clients: Best if you need high-quality LAN based multimedia support. These devices use dedicated firmware in lieu of an OS running on a flash drive, and are designed to handle a single desktop virtualization protocol such as Microsoft RDP/RemoteFX, PCoIP, or Citrix® HDX. Since zero clients have no locally-embedded OS, they have "zero attack surface" making them immune to viruses or malware.

Thin clients with Wyse ThinOS: For those organizations looking to leverage the multi-protocol flexibility of a thin client with the virus-immune security of a zero client, Dell offers Wyse ThinOS. With its extremely small OS base, this category of thin clients is also virus-immune due to its zero attack surface. With no published API or locally accessible file system, Wyse ThinOS has proven to be a popular thin client OS choice where high performance is needed and where security cannot be compromised.

Because the firmware is updated only once or twice a year and because thin and zero clients are managed remotely, IT staffers can be reassigned from "break/fix" work to more strategic projects.





Choosing a VDI endpoint operating system

Once you have selected your ideal device, the final step is choosing an OS that supports your security and user productivity needs. An OS on one end of the spectrum offers more security and easier management, while the other end features more flexibility with broader peripheral support.

Dell Wyse ThinOS delivers the most security and manageability:

Pros

- Inherently virus immune and extremely secure
- Low to no management overhead
- Easy to deploy and works out of the box
- Instant ON with rich multimedia
- Supports both ARM and x86 platforms
- Easy to manage with WDM, Cloud Client Manager (CCM) or "hands off" INI file

Cons

- Peripheral support not as extensive as other OS's
- VDI only – no local application support (eliminating that attack vector)
- VDI only – No local browser (eliminating that attack vector)

Window Embedded Standard or Windows 10 IoT Enterprise provides the most flexibility:

Pros

- Supports unified communications platform such as Lync
- Supports local Windows applications
- Robust peripheral support
- Flexible management options via Wyse WDM & WCM

Cons

- Increases overhead – patching
- Supports x86 architecture only

Linux: in the middle of the spectrum between the most secure and manageable and the most flexible:

Pros

- Supports unified communications platform
- Supports both ARM and x86
- Supports local Linux applications
- Good peripheral support
- Flexible management options
- Easy to manage with WDM or Cloud Client Manager (CCM)

Cons

- Based on general purpose open source (published APIs)

The value achievable by migrating from traditional PCs to more efficient thin and zero clients is easy to appreciate. Your enterprise can benefit from enhanced security, centralized manageability and reduced costs. Choosing the right device and the ideal OS will empower your workers to be as effective and efficient as possible with less downtime and more flexibility. Adding thin and zero clients to a VDI architecture will also provide a higher level of control to your IT department both today and for the foreseeable future.

Choosing the right device and the ideal OS will empower your workers to be as effective and efficient as possible with less downtime and more flexibility.



Dell Recommends the Wyse 5040 Series All-In-One Thin Client

For more information on thin clients, we invite you to visit us at Dell.com/wyse.

