



## TABLE OF CONTENTS

Executive Summary	1
VDI Architectures and Endpoints	2
Five Key Factors for choosing a VDI Endpoint	2
Thin Clients as VDI Endpoints	3
Zero Clients for VDI	5
Zero or Not?	6
For More Information	7

# Zero Clients vs. Thin Clients

## Comparing VDI Endpoint Choices

### Executive Summary

The key driver for companies adopting VDI is the promise of radically lowering the Total Cost of Ownership (TCO) while still delivering a complete Windows-based desktop computing environment. One decision that will greatly influence the success of delivering those TCO savings is your choice of the endpoint or client device architecture.

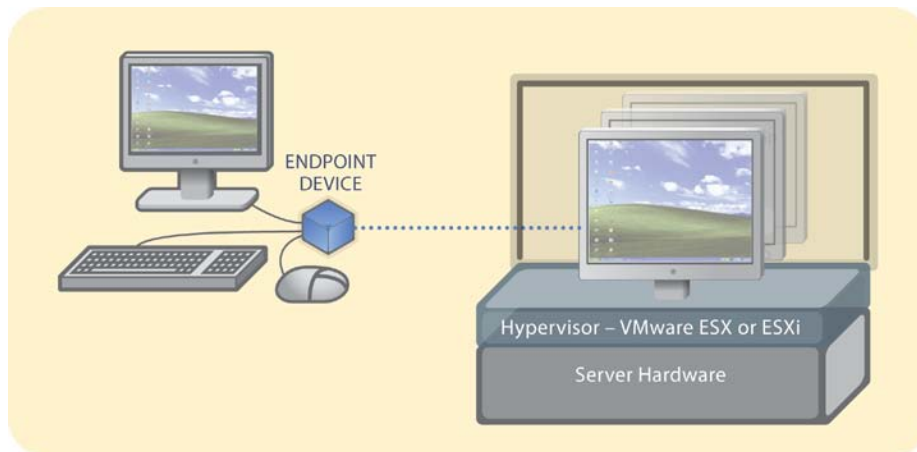
Thin clients used for VDI have been adapted from a prior generation of client hardware originally designed for terminal services and application virtualization. Thin clients come in a wide range of hardware configurations, from limited single-purpose devices with embedded versions of Linux to iterations that resemble a moderately powerful PC running a full-blown Windows operating system.

In contrast, true zero clients have no processing, storage, or software of any kind at the endpoint, and instead centralize all of the processing, configuration, and management on the server in the data center. Zero clients, via radical centralization of desktop computing, can deliver on the promises of VDI by cutting the management and support overhead well below that of other VDI architectures.

This whitepaper looks in detail at how the two dominant VDI endpoint choices — zero clients and thin clients — can influence the cost, resilience, and usability of a typical VDI deployment. It will also provide you with the criteria to understand whether a vendor's offerings are truly zero clients or simply masquerading as zero while not delivering the benefits you need.

**Figure 1:**

VDI endpoints on the user's desks connect to Desktop Virtual Machines running on shared servers in the data center



All of the many technological and architectural approaches to VDI share the common goal of freeing the user's desktop computing environment (and in turn the supporting IT staff) from the constraints and problems associated with deploying, maintaining, securing, and running Windows on physically distributed personal computer hardware.

There are a wide range of VDI architecture choices: what level of

centralization, which hypervisors, management tools, and connection brokers to use; whether virtual desktops are only server-based or also client-based, etc. Possibly the most critical choice is the endpoint types or architecture. This choice will often drive many, if not all, of your other VDI architecture, technology, and vendor choices.

The four main types of VDI endpoints are blade PCs, software clients, thin clients and zero clients. Because they have captured the bulk of the current VDI market, this whitepaper looks in depth at thin clients and zero clients.

## Five Key Factors for choosing a VDI Endpoint

VDI endpoints help deliver many of the benefits of deploying VDI. Five key factors in making a VDI endpoint choice are:

1. **Improve Productivity** – Stateless and management-free VDI endpoints can eliminate the need for IT staff to travel to users in order to resolve problems or perform maintenance. Deploying or replacing an endpoint should never require more than connecting wires and turning it on.
2. **Simplify Adoption** – Endpoints, and their supporting VDI software, should provide essentially the same user experience as native Windows running on the desktop PC they replaced. This not only saves time retraining users and



support staff, but also simplifies supporting the large number of peripherals that users rely on.

3. **Conserve Energy** – Efficient VDI endpoints use just a few percent of the electricity consumed by desktop PCs, cutting substantially the electricity used to power and cool the devices. This savings alone could potentially pay for the VDI deployment in just a few years.
4. **Strengthen Security** – By not storing any data (even temporarily) on the endpoint, the risk to confidential data from malware, hardware failures, or endpoint theft can be eliminated. VDI endpoints should also not present any new security holes that malware could attack.
5. **Slash TCO** – The key overall driver for selecting VDI endpoints is the promise of radically lowering the Total Cost of Ownership (TCO) while still delivering a reliable Windows-based desktop computing infrastructure. In addition to savings from higher IT productivity and energy savings, VDI endpoints should deliver further TCO savings by limiting costs from endpoint hardware and software, systems integration, and user or IT staff retraining.

These five benefits are the key drivers for the return on investments you can expect to realize from deploying VDI in place of traditional PCs. In order to achieve optimal results, it is critical to make careful choices in both the technical architectures and the products and vendors included in your VDI deployment plans.

**Figure 2:**

Thin Clients perform substantial processing on the endpoint device, requiring robust software and hardware

### Thin Clients as VDI Endpoints

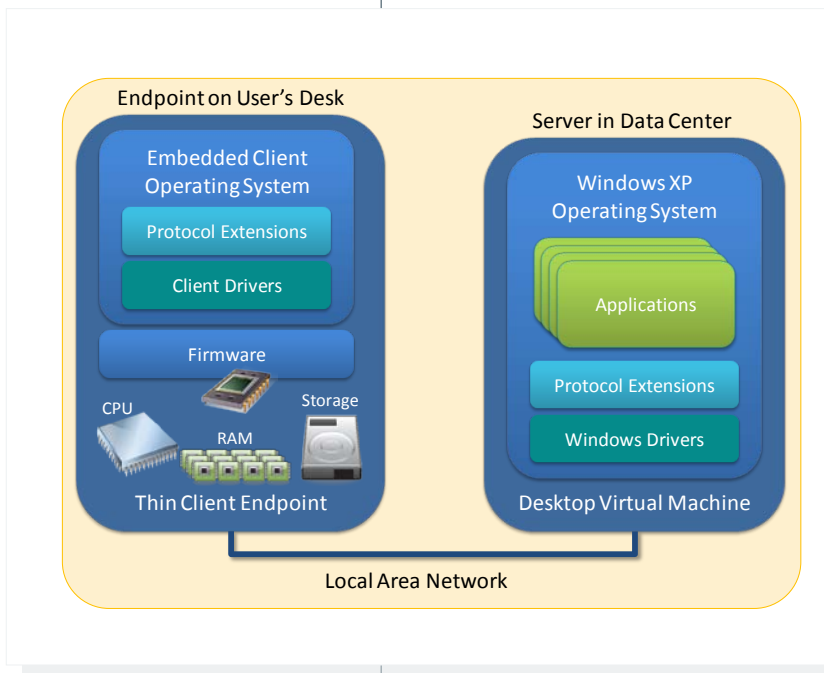
One architecture choice for VDI endpoints is what is commonly referred to as a thin client, the term “thin” referring to the relative “fatness” of a PC used as a

client device. Thin clients used for VDI are often enhanced versions of those used for prior generation terminal services or application virtualization architectures.

A thin client typically includes a CPU, graphics coprocessor, RAM, and local storage like a hard drive, solid-state drive, or simply flash memory. Thin client vendors often offer a wide range of models, from low-cost models for terminal services, to laptop-like mobile clients, ranging up to complex “chubby” models that include multiple DVI video ports, dedicated graphics processors, proprietary compression processors, and even hard drives, making them comparable to low-end PCs in capabilities and prices.

This amount of client-side hardware is required because in addition to the virtualized desktop operating system running on the server, thin clients always

require a second specialized or embedded client operating system running on the endpoint itself in order to function.





Thin client operating systems used for VDI include Microsoft Windows XP embedded (XPe) or Windows CE, although most vendors offer their own proprietary adapted Linux variations originally developed for use with terminal services.

Thin clients typically have fairly extensive firmware and need customized drivers on the endpoint in order to connect the thin client hardware to the embedded client operating system (as well as for support of different management and device monitoring interfaces). These drivers, however, can sometimes be supplemented by protocol extensions that provide services like USB port virtualization to remotely connect the endpoint's peripheral ports to Windows drivers running in the DVM.

Thin client vendors also often provide proprietary management software needed to configure and monitor thin clients. This software is sometimes even embedded, with web-based interfaces, into the thin client firmware.

Strengths of Thin Clients as VDI endpoints include:

- Reduced desktop footprint and lower energy usage is seen when compared to PC desktops (although higher than purpose-built VDI zero client endpoints).
- High-end thin clients have the CPU power needed for client-side processing compression/decompression protocols like PC-over-IP that help with WAN support.
- Past investments in thin clients may sometimes be reused or leveraged for terminal services and application virtualization.
- Terminal services protocols used are familiar to IT staff.
- Where different vendors' thin clients can interoperate, best of breed hardware can be selected to best meet user needs.
- Hardware can be reused for terminal services or other compatible application virtualization projects after failed VDI deployments.

Potential issues using Thin Clients as VDI endpoints include:

- Customers must take on the integration of the thin client hardware with management tools, connection brokers, and VDI protocols from multiple vendors, greatly increasing the risks and fragility of a VDI deployment.
- Deployments with mixtures of thin client models can greatly complicate help desk support and troubleshooting, and may also drive up initial hardware costs.
- Very high skill levels for IT staff are typically required for deployment and maintenance, which can add significant training, staffing levels, or outsourcing costs.
- Thin clients are generally not designed specifically for VDI, leading to compromises and excess endpoint hardware/software to properly retrofit the technology, which greatly add to the management overhead and drives up endpoint TCO.
- Endpoint embedded operating systems require customized client drivers, greatly reducing the range of peripherals (printers, scanners, biometrics, etc.) that are natively compatible and driving up deployment timelines and ongoing support costs.



- Endpoint operating system images often need to be customized for each endpoint configuration, requiring complex OS image management and image backup overhead.
- Thin client vendors charge significant recurring maintenance fees for access to firmware and client OS upgrades or patches, further increasing operating costs.
- Thin clients typically need added licenses to protocol extensions in order to get the terminal services protocols they use (like Microsoft RDP) to perform essential VDI functions such as remote USB peripheral support and rich multimedia display, driving up initial and ongoing operating costs and increasing the complexity and fragility of the deployment.
- Thin client vendors may not be focused on supporting VDI as many get the bulk of their revenue from non-VDI customers.

Thin clients represent an attempt to extend a client-server architecture developed for prior terminal services and application virtualization efforts to support a new architecture delivering full Windows desktop virtualization. While thin clients can work in some settings, the resulting costs and complexity can severely undercut the potential TCO savings that desktop virtualization was meant to provide.

### Zero Clients for VDI

One endpoint alternative to thin client complexity is a zero client, where the term “zero” refers to the complete lack of any client-side processing or management. Many vendors claim that they offer zero clients of one form or another, but these are usually just thin clients that need additional hardware and software for

streaming delivery of the endpoint operating systems, creating a system that is even less “zero” than a regular thin client. The only vendor offering a true zero client endpoint specifically designed for VDI is Pano Logic.

Zero client hardware includes only the simple logic needed for the IP and Ethernet network stack, along with the logic needed to connect to the USB, video, and other peripheral ports on the endpoint.

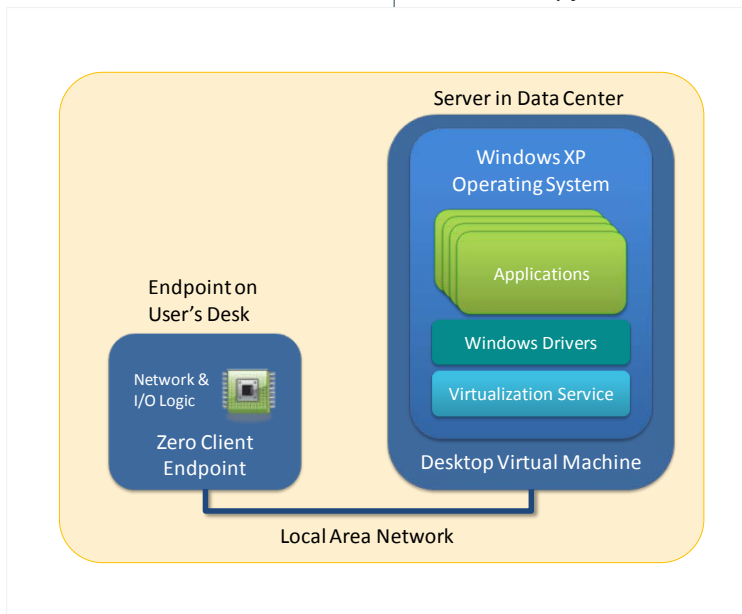
True zero clients omit any client operating system, so neither endpoint-resident drivers nor any other software is required. In fact, lacking a CPU there is nothing in a zero client that could execute any software were it there.

Since there is no need to store any endpoint-resident software or even provide temporary storage of data before it is displayed or passed on to the DVM, zero clients also omit any form of local

storage, whether temporary forms like RAM or more permanent forms like hard drives or flash memory.

While these omissions might initially seem limiting, they actually provide the radical centralization needed to fully realize the benefits of VDI. Unlike the client-server approach to VDI taken by other endpoint architectures, zero clients represent a complete rethinking of the desktop computing architectures that have

**Figure 3:**  
Zero Clients eliminate all processing and software from the VDI endpoint





been in place for the past two decades. Zero clients remove the deployment complexity, hardware/software redundancy, and creeping licensing and maintenance costs that have led to failed VDI pilots and unrealized return on investment of other forms of VDI endpoints.

Strengths of Zero Clients as VDI endpoints include:

- Acquisition costs are lowest of any hardware VDI endpoint architecture because processor, RAM, storage (disk or flash RAM), and other endpoint hardware is omitted.
- No embedded client-side operating system, anti-malware software, drivers, or even embedded firmware is needed, lowering software licensing fees and eliminating the burden of managing software patches and updates for the client OS and drivers.
- Elimination of an endpoint resident embedded operating system means that peripherals never require specialized client drivers to work – just a native Windows driver is required.
- There is zero endpoint management or configuration, saving IT staff time and improving system resilience and reliability.
- Lack of moving parts improves life spans in harsh environments like public spaces and manufacturing plant floors.
- Energy usage is far lower than that of PCs and often as little as one third to one fifth that of Thin Clients (along with little to no desktop footprint).

Potential Issues of Zero Clients as VDI endpoints include:

- They require sufficient network bandwidth, since by definition they do not have the processing hardware and firmware/OS required at the endpoint to execute network compression/decompression algorithms.
- Because they are specifically designed to leanly support a VDI communications protocol, zero clients generally cannot be later repurposed for terminal services or other uses.

## Zero or Not?

The term zero client is often misapplied to thin client endpoints in vendor marketing ploys. True zero client endpoints have no local processing, software, storage, or even any configurations or settings. They are completely stateless and management-free. Zero clients mean zero endpoint management – absolutely zero.

Some thin client vendors have even tried to make their endpoints look “zero” by keeping the client operating system image on the hard disk of a separate “streaming” appliance, requiring that users wait while it is downloaded to the endpoint’s hard disk or flash storage before use. Unfortunately, this only makes the entire VDI architecture from these vendors even more complex and fragile.



To see if vendor claims of “zero-ness” are valid, apply these tests:

1. **Does the endpoint include a CPU of any kind? Any RAM? Any storage devices or moving parts at all?**
2. **Are you forced to configure the endpoint in any way before use?**
3. **Do you need to reconfigure the endpoints before you are able to swap them between users?**
4. **Does the endpoint need to download an operating system image or any software before you can use it?**
5. **Are you not able to use the native Windows drivers that XP or the manufacturer supply to connect to a new peripheral?**
6. **Does the endpoint require you to learn and adopt any embedded management interface or tools?**

If you answered yes to any of these questions then despite the vendor’s claims, the client isn’t a true zero client.

## For More Information

For more detailed information on setting up and managing the zero client Pano Device, go to: [www.panologic.com/pano-device](http://www.panologic.com/pano-device)

For more information visit [www.panologic.com](http://www.panologic.com), email [sales@panologic.com](mailto:sales@panologic.com) or call 650-454-8940 / 877-677-PANO.

Pano Logic, Inc.  
1350 Willow Road, Suite 202  
Menlo Park, CA 94025

© Copyright 2010 Pano Logic, Inc. – issued January 2010 [WP-ZvTC-011910]

Pano, Pano Logic and Pano Button are registered trademarks of Pano Logic, Inc.

Pano Device, Pano Gateway, Pano Manager, Pano Remote, Pano System, Pano Direct Protocol, and Pano Direct Technology are trademarks of Pano Logic, Inc.