

## Wyse Thin Client Remote Access Solutions

*Server-Centric Computing Solutions*

A white paper by  
Wyse Technology Inc.

---

**WYSE**  
| | | |

## THE NEED FOR REMOTE ACCESS

Corporations and government agencies increasingly need to make organizational IT resources available outside the traditional workplace. Whether for home users, telecommuting centers, mobile employees, contract workers, or small field offices, the need to securely access information resources, wherever and whenever, is undeniably growing. Additionally, these remote access points play a critical role in a continuation of operations plan (COOP) if physical access to the regular workplace is not available.

### Challenges

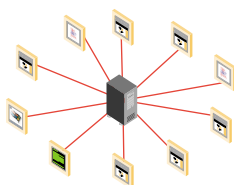
For many IT departments, well planned security strategies fall short when it comes to remote access. Remote access to critical information resources introduces unique challenges:

- How to prevent remote users from introducing viruses or security risks into the corporate network, especially when such users are utilizing their own PCs?
- How to ensure remote computers of any kind are not being used for unauthorized purposes and creating security and support risks, not to mention reduction in productivity?
- How are remote users supported, short of taking on the responsibility of supporting remote PCs?
- How does the IT organization ensure that all of the required application versions are available to the remote user in a timely and cohesive way?
- How can performance be optimized, considering bandwidth may be limited to these users?

Most organizations provide access for remote users through the use of a VPN to maintain security of the data being passed over the network. Some organizations have implemented remote access solutions utilizing Microsoft® Remote Desktop Protocol (RDP) or Citrix® MetaFrame® for server-based computing. There are also several products on the market which provide a remote view of a user's primary PC. Utilizing these approaches, the usual client applications are running remotely, and thus the issues of maintaining applications and OSs on remote PCs are averted, as well as minimizing the requirements for processing power on the remote machines. These solutions can also maximize performance on low bandwidth connections, since only screen views and key-strokes are transmitted, rather than larger files and email attachments, as would be the case with local applications.

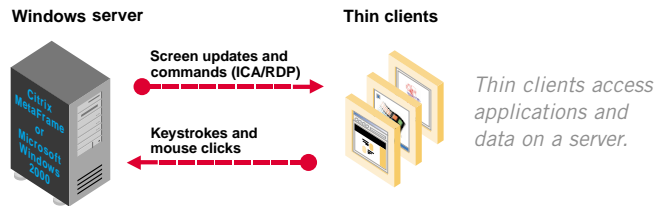
However, this approach alone is only a partial solution to the challenges of secure remote access listed above. There is still a security risk associated with these remote PCs, both from a virus and information security perspective. There is also no assurance that the remote machines will not be used for unauthorized purposes perhaps compounding this risk. And ultimately, the remote user will still need support in the event that the remote terminal application is not loading or operating properly on their machine.

## ENTER THIN CLIENTS



The best overall approach is to merge the above techniques with a thin client, rather than a PC. Thin clients are small information appliances, typically no larger than a cable modem. They provide remote desktop functionality with no hard drive or other moving parts. They can run an embedded browser,

Microsoft RDP client, and/or Citrix ICA client. They have the following benefits over a traditional PC for remote access applications:



- Virus resistance
- They can be configured to be "locked down" so the end user has no ability to modify them and introduce security and support problems
- They can be configured to ONLY work with the designated remote application servers
- They are extremely affordable.

Thin clients can be configured to work with a wide variety of VPNs. They can also be configured to work with cable modems, DSL, and dial-up connections that are commonly used by home workers. In some cases, they are deployed with KVM (Keyboard Video Mouse) switches for home users who already have a home computer and display, thus providing a separate remote access system for work while hardly taking up any additional space in the home office.

## WHAT ABOUT THE INFRASTRUCTURE?

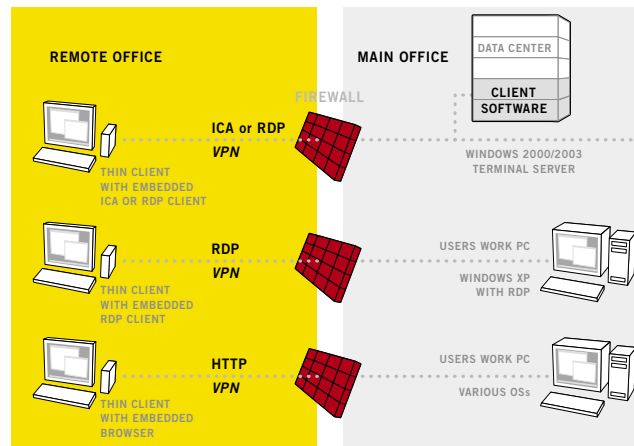
There are various infrastructure approaches to support remote thin-client users:

**Server-Based Computing (SBC):** Remote thin clients can work from applications loaded on server(s) located in a secure datacenter utilizing SBC. Server-based computing involves loading all client applications to run in a multi-user environment in conjunction with Microsoft Terminal Services (which comes standard with Windows® 2000 and 2003 server), or with Citrix® MetaFrame®. Typically 50-70 concurrent users can work from a properly configured two-processor server. The advantage of this approach is that all desktop applications can be easily managed and updated on the centralized server.

**Remote Desktop:** If what is preferred is the ability for users to work remotely with the same user desktop they have at the main office, this can be accomplished using the Microsoft Terminal Services feature built into Windows XP Pro, with RDP. A user can work on a remote thin client in this way, seeing their familiar desktop interface and with access to all local files on their office machine. All processing is in fact taking place on their work machine. As a result, no centralized terminal servers are required.

**Browser-Based Remote Desktop:** Several third party products are available which project a browser based remote desktop view. Products such as GoToMyPC™ and others can work from a variety of host OS environments. Since most thin-client models come with an embedded browser, they can seamlessly work with these kinds of products. Users simply download the software to their office computer and keep their computer running and connected to the Internet. To log on at their remote access location, the Wyse thin clients are configured when turned on to automatically launch the browser to a remote access site address and enter their user name and password. Although a VPN can be used, built-in security features provide a high level of protection, including end-to-end AES (Advanced Encryption Standard) encryption, dual password requirements, user authentication, and screen blanking of their office computer.

## THIN CLIENT REMOTE ACCESS CONFIGURATIONS



### Which Thin Client Is Best Suited for Remote Access?

Wyse offers several thin clients which can be utilized for remote access applications. Which one is for you will depend upon the infrastructure approach you have chosen to use and the type of network connection.

**1000 Series:** The Wyse® Winterm™ 1000 Series is the lowest cost option. They can be used in a server-based computing or remote desktop environment. However, they do not allow for VPN or dial up network connectivity.



**3000 Series:** The Wyse Winterm 3000 Series provide a good option for remote access. They can be used in a server-based computing, remote desktop, or browser based remote desktop environment. They can utilize external modems, and can be used with the Microsoft VPN.



**9000 Series:** The Wyse Winterm 9000 Series provide the most flexible option for remote access. They can be used with server-based computing or remote desktop environments. They have a full function Microsoft Internet Explorer browser if a browser-based remote desktop is used. They can be configured with internal PCI-based modems if required, as well as many VPN clients.

### WYSE INTEGRATED SOLUTIONS FOR REMOTE ACCESS

Wyse Technology, the world's leading provider of thin clients and server-based computing solutions, has extensive experience in these remote access approaches. Winterm thin clients can be custom configured for your VPN, security lock down parameters, and infrastructure preference. Additionally, Wyse, in conjunction with our network of partners and integrators can provide a complete turnkey remote access solution.

### LEARN MORE

Visit us on the web at [www.wyse.com](http://www.wyse.com) or call 800 GET WYSE to get a risk-free trial of our world-leading Winterm thin clients today.