



Command and Control to Protect and Serve: Wyse Technology Server-Centric Computing Solutions

A white paper by
Wyse Technology Inc.

WYSE
| | | |

EXECUTIVE SUMMARY

As government functions become increasingly information based, the technology infrastructure of a government agency provides the foundation for smooth and secure operations. Each day, government workers tap into mission-critical applications and information to accomplish their daily tasks. Whether they provide healthcare at a VA hospital, perform maintenance at an Air Force base, or work with secret information on a classified network, they count on technology to make information access seamless, secure, and reliable.

Thin client, server-based computing solutions give IT managers and government CIOs a foundation for integrated and classified access without compromising security or delaying updates and maintenance. The rise of Windows®-based and browser-based applications caused many agencies to transition from expensive and inflexible mainframe systems to the client-server architecture with networked desktop and laptop computers for access. While personal computers gave workers access to a GUI interface and popular productivity tools, they also created an IT support and security burden for agencies. With increasing concerns about information security and threats to network and computing systems as well as physical government buildings, agency IT professionals are looking for a better enterprise architecture.

Wyse® Winterm™ thin clients combined with Wyse device management software offer agencies and the contractors who support them a high-performance, robust technology solution. With applications and data centralized on secure servers, IT managers have more control over configurations and can respond quickly to virus updates, software updates, and new IT mandates. Because thin clients have no hard drive and do not store any data locally, security risks are greatly mitigated on sensitive or classified networks. In addition, remote offices can be set up quickly and efficiently for telecommuters, or to ensure continuation of operations (COOP) in emergency situations.

This white paper is for IT managers and CIOs in government agencies who are interested in robust technology solutions to improve manageability, security, and access to mission-critical applications and data. As the information age comes upon government agencies in the midst of threats to safety and security, the ability of an agency to respond quickly and efficiently to citizen needs has become an imperative for IT.

TODAY'S IT CHALLENGES FOR GOVERNMENT AGENCIES

IT managers and government CIOs balance the availability of information with the protection of it to support their agency's mission. Technology is both the cornerstone of improved government productivity as well as a target for attack. Amid these competing

challenges, budgets fluctuate with changes in the economy and political agendas, making IT planning uncertain.

Critical Mandates and Essential Updates

One of the most consistent challenges for government IT departments and providers is the constantly changing requirements and mandates for technology use. A mandate may require the implementation of a security patch, a new version of an application, or a new configuration to meet enterprise requirements, IT managers have to respond quickly to mandates that are sometimes overlapping, even contradicting, and very often, unfunded. With thin clients, IT managers make the changes on the servers and they are available on all thin clients within hours to comply quickly, efficiently, and in a verifiable way. The same update to PC workstations requires staff members to assess whether or not every workstation can accept the change, then the change is made, then it must be verified.

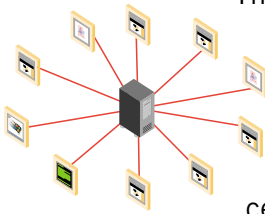
Privacy and Security in a Networked World

Sensitive or classified data within government requires protection from unauthorized access and theft. Desktop computers or laptops with the capability to store sensitive data on their hard drives increase the risk of outside intruders. When data is available on computers with portable media and network access, authorized users can save and copy files or send them to unauthorized recipients. Users with computers that enable them to download, install or reconfigure their setup may inadvertently open vulnerable access points or launch virus attacks. By shifting information and applications from desktop devices to servers, thin-client computing shifts the burden of protection to a more centralized and manageable location.

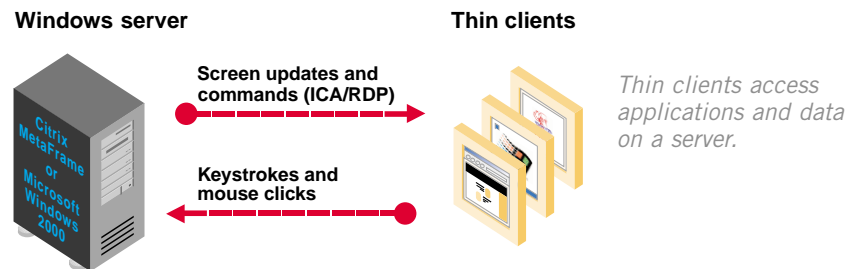
Ready for "What If"

Until recently, continuation of operation (COOP) plans have focused on data center and network redundancy and ignored the client. Every government agency today must think through the "what if" scenarios. Even if the data center and the network are available, what if we cannot get into our building? What if power or communication services are cut at a location? How will we recover and continue operations as quickly as possible? Because no data is ever stored on a thin client, a worker has continued access to mission-critical data and applications, regardless of access to a particular, physical thin client device. Thin client architecture meets new standards of survivability, resilience and disaster recovery with quick setup and centralized off-site or multi-site server farms.

THIN CLIENT COMPUTING SOLUTIONS



Thin clients began as simple terminals using a multi-user Windows platform to connect to centrally managed, secure application servers running either the Citrix ICA or the Microsoft RDP. They gave workers fast, reliable access to Windows-based applications without the management and security issues of a personal computer. Data processing occurs on terminal servers connected directly to data servers; only key strokes, mouse clicks, and screen images travel the network, requiring relatively low network bandwidth. Users simply log-in from any thin client on the network to bring up their applications and information. Today's thin clients have become the standard for access in hospitals, financial institutions, shipping companies, retail stores, and many other industries.



Wyse® Winterm™ Thin Clients

Wyse Technology pioneered thin clients and has the largest market share worldwide. Winterm thin clients range from simple thin clients with the basic protocols needed to connect to terminal servers to powerful and flexible thin clients with local application processing, additional I/O ports, and optional local peripherals. Platform options include Wyse's Blazer client technology, Linux, Windows CE, NET and Windows XP. Winterm thin clients combine the security of a mainframe with the interface and flexibility of a desktop computer, providing access to legacy mainframe applications, secure web-based information, and Microsoft Outlook, Word, and other PC applications. Access features include password protection, smartcard access, and biometric security sensors.

Wyse™ Rapport® Software

Every Winterm thin client includes Wyse Rapport device management software to change, upgrade, and assess all thin clients on the network domain remotely. The administrator has the option of downloading firmware, embedded applications, and other features to the thin clients at any time, in any order, and to any grouping of terminals. Using server-based policies and utilities, administrators can implement new users, IP addresses, locations, permissions, security levels, and peripherals.

BENEFITS FOR GOVERNMENT AGENCIES

Information not only plays a part in the daily functioning of government operations, it has become essential to national security. Government agencies have realized the power of integrating information systems to enable cross agency reporting and access. The new enterprise architecture favors compatibility, scalability, and security. Wyse thin-client computing solutions give agencies the command and control of information they need to protect and serve.

Centralized Management, Support, and Control

Centralized management of updates and software deployment enables agencies to respond quickly and efficiently to mandates. When one government healthcare agency was required to update screen settings on all desktop devices, the IT department manually configured one desktop and pushed it out across the network to all Winterm thin client devices. Not only did the managers respond, but they could track and report on the results, certain that every desktop on the network had the new configuration.

Centralized control also improves protection against viruses, worms, and other attacks. The technical team keeps security patches up-to-date on the servers to prevent disruption for users. Thin clients require patches less frequently than PC's, but if they are required Rapport software pushes the new updates out to all thin clients.

Secure Desktop, Data, and Devices

Thin clients shift security requirements from the computer to the network, making security more manageable and robust. Access is controlled through multi-level identification and authentication, and no data or application resides on the access device. If a thin client fails or is stolen, nothing is lost or compromised and a new thin client device is simply swapped into its place. Servers are regularly backed up and redundant systems in multiple sites support continuation of operations.

Easy Access, Anywhere for All Users

The benefits of thin clients are not limited to administration or security professionals; users find thin clients fast, easy-to-use, and more reliable than PCs. With centralized support for patches, updates, and archiving, users can count on up-to-date systems, consistency from one thin client to the next, and frequent backups. Thin clients boot up faster than PC's and applications are processed on the servers, maximizing and leveraging processing power across the organization, improving performance on every desktop.

Because users log-in to servers for their mission critical data and applications, they are not tied to a specific location in a thin-client environment. A nurse can open an application and bring up patient records at the nurse's station, then move to an exam room and access the same desktop without taking time to reload applications or refind records. An

Air Force Base may provide technicians with a smart card for access from multiple locations in a maintenance bay. When they insert their card, their specific session appears with interfering with other technicians.

Replace and Restore Services

Many contractors tailor thin clients to fit directly into their technology solutions. They set up new users and new locations on the servers, and then ship thin-client devices to remote or even temporary locations. They are unpacked, plugged in, and turned on. The thin client connects through the network to the servers for the latest configuration.

Lower Purchase Price and Total Cost of Ownership

With server-centric computing an agency builds on their technology investment each year. Thin clients cost less per seat than laptops or desktop computers with the same applications and Windows-based interface. They connect through most standard networks: 10MB Ethernet, 100MB Ethernet, Wi-Fi, even dial-up and wireless WANs. Because thin-client devices typically have no moving parts to fail and applications are managed on servers, thin clients have the lowest total cost of ownership (TCO) of any computing device used today.

The worksheet below shows three cases for calculating TCO savings with thin clients using high, medium, and low TCO estimates for PCs and three different prices for thin clients. Even the most conservative estimates (Low) result in technology savings within the first year of deployment.

Return On Investment Expectations

	<u>HIGH PC</u>	<u>MEDIUM PC</u>	<u>LOW PC</u>	
PC Cost/Year	\$14,000*	\$10,000*	\$9,000*	A
TC Savings	57%	35%	20%	B
TC Savings/Year	\$7,980	\$3,500	\$1,800	C=A x B
Savings/Month	\$665	\$292	\$150	D=C/12
Cost of TC	\$399	\$525	\$1,099	E
Payback (months)	0.6	1.8	7.3	F=E/D
First Year ROI	1900%	567%	64%	

* Gartner Group Estimate

Agencies report that they can support more thin-client devices in more locations with fewer IT staff than an environment of desktop computers and laptops. By consolidating management in key locations, they can hire the best, most qualified people to support local and remote users.

One agency measured help desk call frequency and call length for thin client and PC users within the same computing environment. They found that the help desk received 50 percent fewer calls from thin client users than PC users and those calls lasted half as long. Because a thin client has no local configuration and the help desk can shadow the user, they can respond more quickly and effectively to the help desk call.

PLANNING FOR THE FUTURE

Information technology has the potential to streamline operations and improve service, helping government agencies meet their mission of high quality, prompt and seamless service to citizens. Wyse Winterm thin clients and Rapport management software open the door to access for government agents and workers without compromise.

Hundreds of thousands of Wyse Winterm thin clients have been deployed throughout government agencies and corporations worldwide to support easy access to critical information and applications. With server-based, thin-client computing systems, IT managers and government CIOs rest assured that their services will be available and operable.

