

How CLI Windows CE .NET Thin Clients Can Reduce IT Security Risks Vs. PCs Or Other Devices

Use of CLI thin client devices instead of PCs or other devices can dramatically reduce the security risks present in any IT environment. To fully understand this benefit, it is important to understand what server-based computing is, and what CLI thin clients are.

Server-Based Computing

The cornerstone concept behind CLI thin clients is server-based computing, which is sometimes referred to as server-centric, centralized, application-server, or client-server computing. In server-based computing, all applications are deployed, supported, and executed at the server, not at the user desktop. All data is stored on the server. Only keystrokes, mouse clicks, and the screen images travel across the network (or the Internet). All applications are displayed on the desktop device. This desktop device can be a text terminal, a Mac, a PC, terminal emulation software, or a CLI thin client.

CLI Thin Clients

CLI thin clients are simple devices that are used for information display. CLI thin clients do not “run” applications, but can display any application containing graphics or text information. Applications look the same as the original. CLI thin clients have no local hard disk, floppy, or CD storage, and no fan or other moving parts. Most CLI thin clients have a local Windows CE .NET operating system. Their use brings many benefits, including a low Total Cost of Ownership, easy administration, high reliability, long useful life, and low power consumption. But the use of CLI thin clients also brings the benefit of reduced security risks.

Reducing Security Risks

The use of CLI thin clients can reduce security risks in many ways.

CLI Thin Client Devices Reduce The Number Of Potential Virus Entry Points Into An Organization

Computer viruses or worms are spread in a number of ways, including through infected files located on local hard or floppy drives. Unlike PCs, CLI thin clients have no local hard or floppy drives, so viruses cannot enter in these ways.

CLI Thin Client Devices Are Nearly Virus Resistant

CLI thin clients have a local Windows CE .NET operating system. This operating system is stored locally in something called flash memory, a non-volatile memory system. A PC's operating system is typically stored on a local hard disk. Unlike a PC with a hard disk, CLI thin clients do not allow information to be written to the flash memory except for configuration changes made by the user. In addition, since applications run on the server and not on the thin client, if infected files such as email attachments are inadvertently opened, the virus is contained on the server, and not spread to any other desktop devices on the network such as PCs. This can avoid costly patches and / or repairs. Finally, on boot up, the local operating system used in CLI thin clients is loaded from flash memory into RAM, where it then executes. In the remote situation where a virus has infected the operating system executing in RAM, the CLI thin client can simply be turned off and then back on to restore the original local operating system stored in flash memory.

CLI Thin Client Devices Are Resistant to "Hacking"

CLI thin clients have some exclusive security features, including user passwords and lock out capability. Attempts to alter the thin client's local operating parameters, or unauthorized access to application servers, can be thwarted by password protecting the thin client.

CLI Thin Client Devices Are Not Prime Targets For Theft

CLI thin clients do not "run" applications, they simply display application information. They also are "locked-down", "sealed-box" devices, with no local hard disk or CD drives, and minimal local flash and RAM memory. Since they require the application server in order to perform their function, and are only really used in commercial environments for commercial applications, they are typically not subject to theft or tampering the way PCs are.

CLI Thin Client Devices Keep Data Secure and Private

Unlike PCs, CLI thin clients have no local removable media such as floppy or CD drives. Valuable and sensitive information and data cannot be removed from an organization through a CLI thin client. Plus, since all data in server-based computing is stored on the server, data backups can be performed more efficiently and easily on the server than can be performed on multiple distributed PCs. In addition, CLI thin clients support software protocols that keep data secure during transmission and reception, including authentication services such as SSPI, NTLM, Kerberos and SChannel (SSL/TLS); cryptography services such as certificates; SOCKS, and secure ICA.

CLI Thin Client Devices Permit IT Staff to Focus Security Efforts On The Server and Network

Since the use of CLI thin clients reduces overall security risks, the IT and System Administration staff can spend less time trying to secure every desktop, and more time in efforts to secure the server and the network. Methods such as anti-virus software, Virtual-Private-Networks (VPNs), firewalls, and educating end users on proper practices and procedures, when combined with server-based computing and CLI thin clients, can make security problems a thing of the past.

For more information, visit the Computer Lab International web site at www.computerlab.com, or send email to info@computerlab.com, or call 1.800.727.5250 in the US, 1.714.572.8000 elsewhere.

Computer Lab International™ is a trademark of CLI, Inc. All other trademarks are the property of their respective owners.

###