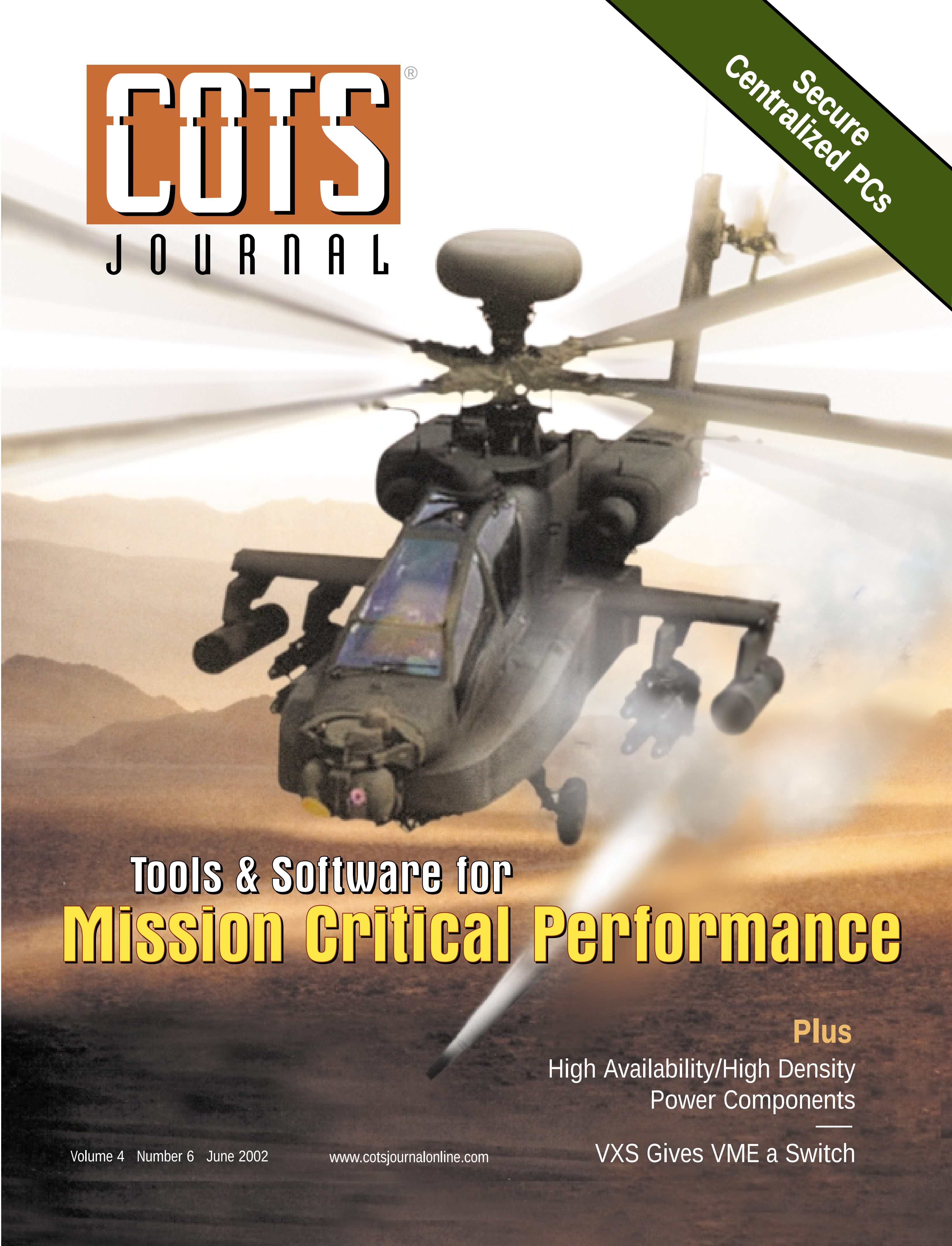
COTS® JOURNAL

Secure Centralized PCs



Tools & Software for Mission Critical Performance

Plus

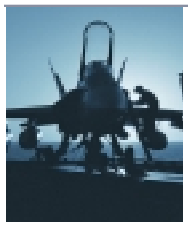
High Availability/High Density Power Components

VXS Gives VME a Switch

Volume 4 Number 6 June 2002

www.cotsjournalonline.com

COTS View



Increasing PC Security with a Centralized Client Blade Architecture

With heightened security everywhere, PCs and their open standard LANs present a vulnerability hole that can be plugged with a centralized client blade architecture, leaving only the traditional I/O devices including monitor, keyboard and mouse on the desk.

Carsten Puls, Director of Strategic Development, ClearCube Technology

Managers responsible for IT in government and military installations have always had security as a high priority. Today, more than ever, government organizations need better tools and methods to fully control and secure their sensitive networks, data, and the physical assets that store and process the data. Unfortunately, the proliferation of distributed box PCs runs counter to this need for better security. While conventional computing approaches are difficult to secure, newer centralized blade architectures based on standard PC technology promise very high levels of security.

Three Types of Security

Security concerns in government IT groups focus on three key areas: network security, data security and physical asset security. Network security involves controlling the access points to a computer network that carries sensitive information. In many military bases two networks are run: a standard network for base personnel that is relatively easy to access, and a secured network that only certain personnel can access. The secured network carries classified information and therefore has minimal access points and very few portals to the outside world.

Data security deals with the means by which electronic files can be removed from a computer—either through the network or through portable media such as floppy drives and CD-ROMs. Data security is also concerned with the ways in which detrimental files or viruses can be loaded into the computing system.

Finally, physical asset security involves the portability and removal ease of computing systems such as whole PCs or internal components such as hard drives. The concern here is not so much the value of the assets alone, but the value of the *data* that may be stored on the asset.

Distributed PCs Compromise Security

Box PCs spread throughout an organization can seriously undermine an IT manager's ability to fully control and secure critical information and computing assets. For example, we have all seen how potentially disastrous it can be when a single hard drive containing secret nuclear weapons information from Los Alamos goes missing. Ultimately, in a world where information is one of our most effective weapons against enemies like terrorists, securing and controlling that information becomes paramount.

So the problem we are faced with can be summarized by two conflicting points. Firstly, one of the best examples of a successful implementation of COTS technology in the military and government is commercial box PCs. But to the contrary, the inherent nature of distributed box PCs compromises the security required in military and government installations. Finding the right balance can be difficult (Figure 1).

Why are PCs a Great COTS Technology?

One can find hundreds of examples to support why commercial PCs are one of the best COTS technologies benefiting military and government operations. Productivity gains from standard PC software applications such as word processors, spreadsheets and e-mail make our tax dollars go further. The flexibility of standard Windows operating systems lets military personnel choose from thousands of application-specific software programs.

The low price/performance ratio of PCs is but a fraction of what application-specific computing hardware costs. Even train-

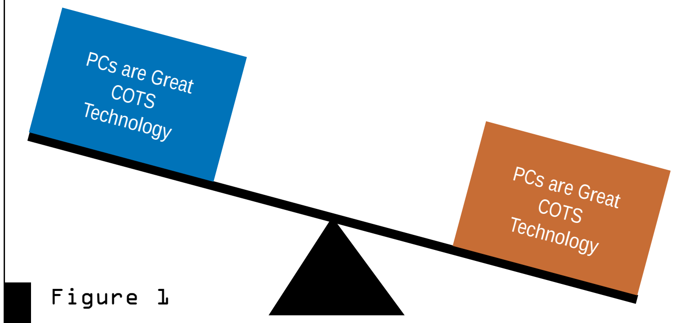


Figure 1

PCs in secure applications involve a tradeoff between ubiquitous desktop computing capabilities and compromised data security.

ing costs for military and government personnel are minimized when using standard commercial operating systems on PCs that are already familiar to new recruits. So there is no doubt that PC technology makes a lot of sense.

Why are PCs Inherently Insecure?

The great benefit of PCs is that they bring high-performance computing power, storage, I/O and flexibility right to the end user. This benefit, however, results in a significant reduction in both data and physical asset security. With distributed PCs, sensitive data is very easily stored on a hard drive that can be in any location throughout an organization. Furthermore, that data can easily be transferred to portable media such as floppy disks, CD-ROMs and ZIP drives. It is also very easy to remove an entire hard drive from a box PC containing as much as 100 Gigabytes of data. This equates to the text in about 20,000 issues of *COTS Journal*—all in a device that easily fits inside a coat pocket!

The ease with which data is removed also applies to the ease with which someone can load unwanted software that may contain viruses. In addition to limited data security, physical security can be compromised since the other valuable assets inside a PC are easily stolen. For example, memory and processors can easily be removed from computers distributed throughout an organization.

Finally, network security is also a limitation because network access points are distributed to each desktop. So even if a particular desktop has its floppy and CD-ROM drives removed, this doesn't prevent someone from bringing in a notebook computer with drives and connecting it to the network port. Then they can upload or download software at will.

Conventional PC Security Measures are Merely Patches

Government organizations have several options when it comes to increasing the security of their PCs. Most of these options, however, are "band-aid" approaches that fail to go to the root of the PC problem. For example, government organizations can conduct scans and perform random searches on employees as they leave the facility. This method is only as good as its execution, which is expensive and intrudes on the privacy of individuals. It is also a very time consuming approach. Furthermore, this type of manual security service is subject to human error and can easily be breached.

Government IT groups can also limit what kind of data can be stored on a PC. Utilizing central file servers for all data storage is an excellent approach. Again, this is only as effective as the actual execution of a policy. End users can easily make exceptions and still store data locally. The breaches always occur with the exceptions. If data is stored locally then the physical assets can be secured with cables and locks. This is a common practice in public areas and training centers where the user turnover is high. Physically locking down the assets, however, is expensive and difficult to monitor and manage. Conventional cables and locks can be cut and picked if someone is really motivated.

In order to limit the I/O flexibility, some installations use PCs without a floppy drive or CD-ROM drive installed. However, this method does not prevent someone from plugging in a portable USB drive to retrieve/archive data. Password protection can be used to control some security aspects including the ability to add/remove USB storage devices to a computer. However, this is only as secure as the password—something that end users can often obtain without too much difficulty. Box PCs do not have any hardware lockouts that prevent certain USB devices from being connected—security is just based on software passwords.

Conventional Thin Clients Add Security but Trade-Off Performance

One alternative to using box PCs is to use thin clients. An ideal thin client is one where all processing and data storage is centralized and only a small, minimal device resides on the user's desktop. Thus, no data or other valuable assets are distributed throughout the organization. An ideal thin client will also deliver the full PC experience to the desktop without compromise. This centralized approach increases security and also improves manageability since systems can be serviced in the IT center without having to go to individual desktops.

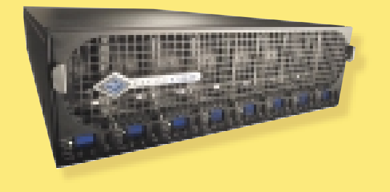
Today's most common thin client architectures still use Ethernet as the method to connect the centralized processing and data storage to the end-user devices. In these systems Citrix or

Securing Desktop PCs Through a Thin Blade Architecture

The client blade architecture is composed of several key hardware and software components. The table below describes and shows the components used in the client blade implementation offered by ClearCube Technology.

CPU Blade

A rack-mounted Intel-based computer that delivers services to each desktop from a centralized location. Each user has their own blade with processor, memory, HD, and power supply.



Cage

Houses up to eight CPU Blades in a 3U-high enclosure. A standard 42U 19" rack holds up to fourteen Cages, or 112 CPU Blades.

C/Port

A small videotape-sized unit that connects the keyboard, mouse, video, audio, and USB devices on the desktop to the CPU Blade via Category 5 cable.

Limited Peripheral Connectivity	Typical thin clients do not support connection of peripherals other than keyboard, mouse, and video.
Limited Software Flexibility	Software applications have to specifically support the thin client, shared processor approach— thus users and IT administrators do not have access to the broad array of software applications available for standard PCs.
Poor Scalability	The busier the clients become, the slower the server responds to requests since a single server is shared among dozens of users.
Single Point of Failure	Disruption of service to all users is possible when a server goes down. To avoid this problem more advanced redundant serving and load balancing software is required—in turn, increasing costs.
Thin Client = Fat Network	The networking and serving demands for thin client are much higher than with a networked PC installation. In turn, operating costs are significantly higher.
Training	Thin client is neither a traditional platform for IT managers or their users. This lack of familiarity requires additional training. IT managers and end users are now required to learn a new operating environment.
Weak Performance	Thin clients have performance limitations that hinder many types of applications. This results in disappointed users because of the sluggish response to keyboard strokes or mouse clicks, and delayed screen updates.

Table 1 Thin client disadvantages limit their applicability to the military/government.

Windows Terminal Server software are run on servers in the IT center. A single server runs the applications and stores the data for dozens of end-user stations through Ethernet connections. The end-user stations do not store data locally and basically just process video, mouse clicks and keyboard strokes. The local unit converts this user I/O information into Ethernet packets that communicate back to the shared server.

This thin client approach provides very good physical asset security since there are no hard drives at the desktops to be stolen. Data security is also strong since thin clients typically do not have floppy or CD-ROM drives. However, network security is still a weak point, since open-standard Ethernet access points are still spread throughout the organization.

Although conventional Ethernet-based thin clients offer additional security, this comes with many trade-offs that most government IT managers are not willing to deal with. Table 1 lists several of these disadvantages including the concept of “thin client = fat network.” Although thin client terminals are often priced below $500-$700, the server computers and networking equipment needed are priced higher than those used in standard PC client/server systems. This is because the networking and serving demands for thin client computing are much higher than with a networked PC installation (hence the term “fat network”). In turn, the service, support and licensing costs of these higher-end servers and specialized software add administrative costs.

Thus, although conventional thin clients add some security, they are really not a viable alternative to PCs because they eliminate many of the key benefits that made PCs an excellent COTS technology to begin with. So how can we have our cake and eat it too?

Client Blade Computing Combines Security with PC Performance

The primary security issue with traditional PCs is not *how* they run and operate but *where* they run and operate. The entire PC security problem can be solved by simply *relocating* the PC assets to a centralized location with a secured connection to the end user. This connection needs to only carry the user’s interface signals (keyboard, video, mouse and USB) from the computer. An end user does not need their hard drive and processor to be physically 3 feet from their keyboard. If the full functionality of the PC can be delivered from 600 feet away—the user is not affected. This is effectively what the client blade architecture does to address physical, data and network security.

In the client blade approach, the PC assets including a Pentium III or 4 processor and motherboard, memory, hard drive and power supply are built into a compact “blade” computer that runs standard operating systems such as Windows and Linux. 1U-high rack PCs or servers with keyboard-video-mouse (KVM) extenders can also be used in a similar fashion. However, a single standard 19” rack accommodates 42 1U-rack PCs whereas blades are available with densities yielding 112 blades in the same space.

A KVM connection from each blade goes out to each end user’s desktop over standard Category 5 cable (the same cable formerly used for Ethernet). The cable connects to a small device that is about the size

Blade Switching Backpack

Attaches to the Cage and provides remote switching of CPUs to spares for maximum availability.

ClearCube Management Suite

Software that enables IT managers to monitor, control and switch CPU blades via the Internet.

of a video cassette tape. This device provides the connections to video, keyboard, mouse, speakers and USB devices. Effectively, the Category 5 cable is being used as a long distance (600+ ft) extension cord to the user's interface devices. Thus, each user still has full PC functionality with their own processor, memory and hard drive, but these assets are now centrally located—where they can be secured. The result is unprecedented data security, physical asset security *and* network security without compromises.

Assets and Data are Secured in a Central Location

With client blade computing IT managers can rest easy knowing that all data and assets are secured in a central data center under lock and key. There is nothing for an end user to take from their office that contains any data or holds any valuable assets. The device at the desktop usually costs less than $250 and does not store any data. Furthermore, the desktop device typically has no moving parts and often has a mean-time-between-failure (MTBF) of over 250,000 hours making support calls to the desktop a thing of the past.

The USB ports on the desktop device provide flexibility to connect to a wide range of peripherals such as printers, scanners, headsets and cameras. However, because security is a key aspect of the client blade architecture, connection to USB mass-storage devices (floppy drives, CD-ROM drives, ZIP drives) can be locked out by the IT manager via a hardware setting on the centralized blade. This prevents a user from downloading any data to a portable medium thereby increasing data security. Figure 2 compares PCs with the thin client approach and client blade computing to demonstrate the effects of centralization on asset, data and network security.

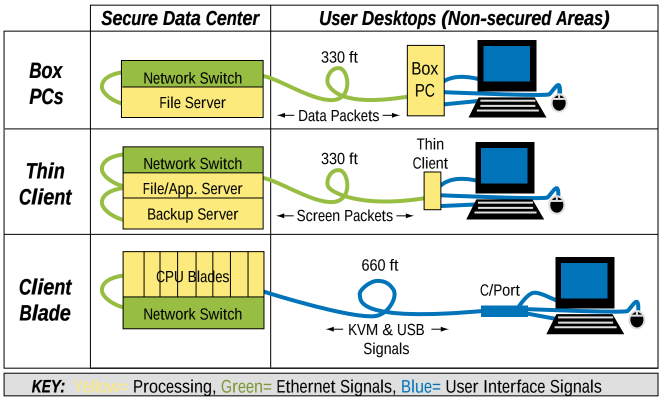


Figure 2

Unlike other approaches, the client blade architecture does not put network data or computing assets in the unsecured end user areas.

Network Access Points are No Longer Spread Out

A key security benefit of the client blade architecture is the fact that Ethernet ports are not spread throughout the organization. With "secured" box PCs that do not have floppy or CD-ROM drives, a user with a notebook computer could easily disconnect the box PC from the Ethernet outlet and then connect their notebook computer which does have portable media. In this way, every Ethernet port becomes a potential security breach.

With centralized client blades, the ports at a person's office or cubicle do not have Ethernet, just the keyboard, video and mouse signals to which a notebook computer cannot connect. With a client blade approach, all the Ethernet connections and traffic are confined to the data center—network runs are only a few feet long because they only need to run from the blades to an adjacent network switch.

Additional Benefits Lower Support Costs

In addition to high security, client blade computing delivers several other key benefits. With centralized assets, deployment and service become very straightforward—resulting in better manageability. Trips to individual user's desktops are no longer necessary. By integrating remotely controlled hot swap technology into the rack of client blades, one user can be switched from one blade to a live spare in an instant, resulting in high availability for clients.

This means that downtime can be measured in minutes and seconds, not hours and days. The small desktop device frees up space and eliminates the heat and noise generation common to box PCs. Effectively this architecture "clears the cube" of the box PC. The improved security and the other benefits previously described ultimately translate to a lower cost of operation and ownership for computing assets. Many of these cost savings come from more efficient use of IT personnel. Figure 3 shows an example of the client blade architecture as available from ClearCube Technology. The sidebar describes each component of the architecture in more detail.

Ultimately, the client blade approach merges the best of PC technology with the ideal concept of a thin client to result in a truly secure, high-performance computing solution. This approach is already being implemented on military bases throughout the US where security of information is of critical importance. Other applications such as rapid deployment and setup of field command centers are being developed to take advantage of the secure aspects of centralized client blade computing. ▮▮

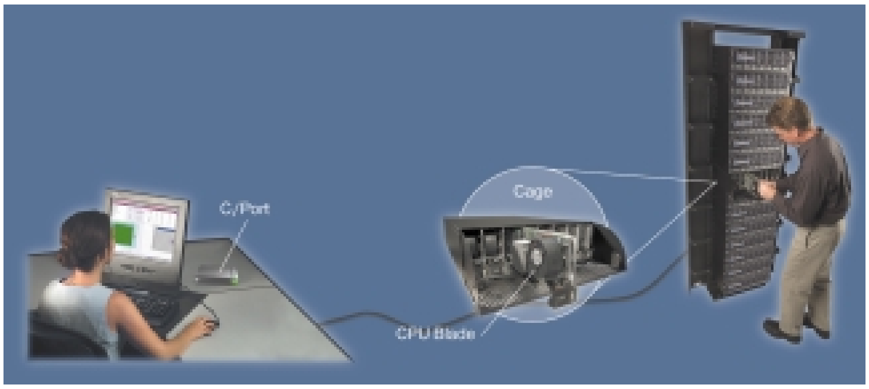


Figure 3

Client blade computing increases security because all data, physical and network assets reside under lock and key in the centralized data center.

ClearCube Technology
Austin, TX.
(866) 652-3500.
[www.clearcube.com].