White Paper

Smart Terminal Architecture with Secure Hosts (STASH):

A New Evolution in Smart Computing for the Enterprise

IBM
VICOM Infinity
Intellinx
Raytheon Trusted Computer Solutions
Virtual Bridges
CSL International

STASH Consortium

April 20, 2012

Executive Summary

This paper introduces the concept of the Smart Terminal in a Secure Host. The Smart Terminal consists of many of the pervasive computing devices listed above with military grade security on the end user interface combined with a secure and resilient back end hosting environment.
The IBM mainframe, the first widely successful and plug compatible commercial computer was widely known for it's green screen Dumb Terminal 3270 interface which was centrally managed by an IT staff. The advent of the IBM PC and later, pervasive computing devices such as smart phones, tablet computers, cell phones, ATMs and kiosks have replaced those dumb terminals as the front end or human computer interface for most business and government related transactions today. The dilemma is that the end user becomes the systems programmer for those devices. They are susceptible to security problems (viruses), loss/theft and breakage. Identity theft and fraud are other results of insecure devices, which may not impact a consumer, but cause tremendous costs for businesses to recover from or mitigate those risks.

Many times, a business believes that they need to spend more to get this level of security. Through advancements in technology and collaboration across vendors, it is the goal of the Smart Terminal architecture to:

- Reduce initial acquisition costs by taking some costs out of the solution
- Reduce operational costs and deployment risks
- Improve the security and resilience of the deployed solution
- Leverage existing investments wherever possible
- Provide investment protection and continued cost benefits through future technology deployment

A multi-functional team across IBM, Raytheon Trusted Computer Solutions(RTCS), Virtual Bridges, CSL International, Intellinx Software and Vicom Infinity Inc has come together to demonstrate the architecture associated with Smart Terminal computing in a secure hosting environment. Each of these businesses brings a component of the overall solution to market. Each product has been generally available to customers. RTCS delivers its proven front end processing Trusted Thin Client®(TTC) offering that is widely deployed across ten's of thousands of US military, intelligence agencies and other governments' desktops. Virtual Bridges' VERDE provides desktop management and provisioning. IBM provides a secure and resilient hosting environment for desktops within its zEnterprise Bladecenter Extension (zBX) and z/VM. CSL International provides their customer proven CSL-WAVE product to manage the virtual machines using an intuitive interface. Intellinx zWatch provides a user activity monitor. Vicom Infinity brings a variety of simplication software and experience with many of the world's largest financial institutions.

The Desktop Computing Conundrum

With the 30+ year evolution of the Personal Computer, in most environments, the end user is the Systems Programmer. Software installation, patches, virus detection and recovery actions are undertaken by the end user. Central administration can help by running tools to check for compliance and to push patches and software to the end user, but ultimately, the end user has predominantly held the ultimate responsibility. When a central organization has greater control, they are still limited by physical access to the managed PC. If it is removed from the network, then service updates cannot be maintained.
In many businesses, such as in financial management and intelligence organizations, multiple personal computers may be utilized because different networks are required to separate access points for end users. Within financial management, customers may access a trader via one network and one PC for the trader, while the trader processes the trade on another network, which the client is not allowed to be a part of, to avoid fraud or data theft. Similar network and PC compartmentalization is done within the military and government intelligence agencies.

In large enterprises, the volume of PC's takes up tremendous energy and cooling. The upgrade of technology, which may occur every three years or so, is extremely time consuming and labor intensive.

While an end user may feel they are getting their computational needs satisfied, the business may not feel the same as those end users as the PC may only be utilizing 5% of its capacity. The rest of the time, that volume of computational resource, at a corporate level, is sitting idle or inaccessible for other usage.

The Smart Terminal Control Unit

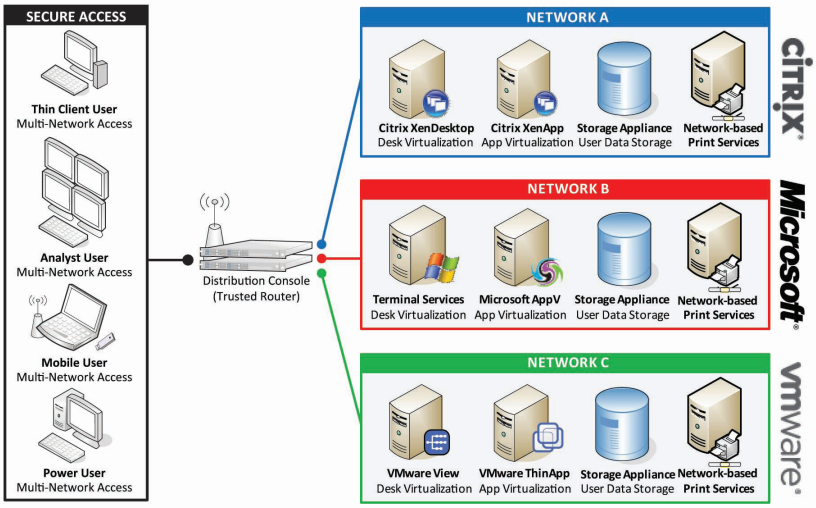
Virtualization of server images began a few years ago in the x86 world. thin client computers were introduced, but they had not been widely deployed until virtualization could occur on back end servers to reduce deployment costs. A wide variety of thin client computers, utilizing standard protocols, are available. However, many of these thin clients are managed within a desktop domain and not necessarily as part of an end-to-end enterprise workflow. The Smart Terminal aims to facilitate that end-to-end management.
RTCS works with a variety of thin client computers. They replace the firmware of those devices with a secure Linux® core and their own middleware. This core disables certain functions such as cut and paste operations between graphic windows and applications. It also labels all traffic by application to classify the work that is being executed so back end servers can properly manage those connections. This classification and compartmentalization of workloads enables a form of screen consolidation to occur at the desktop. The result is a "disposable, stateless" device that uses a fraction of the energy and space of multiple PCs. Should there be a problem, it can quickly and easily be replaced by an end user. This becomes the foundation of the Smart Terminal.

And whether a business or agency has a single network or multiple networks, the RTCS TTC is the technology to use. Financially, it is similar in price to alternatives. However, operationally, it offers a variety of operational savings. All updates to the firmware are delivered from a centrally managed Distribution Console. This reduces the risk and hardens the front-end terminal. Other offerings require software updates be triggered by the end user and those same end users can change the configuration, which puts the terminal at risk.

lsantalucia@vicominfinity.com

Multi-Network Access
Secure Information Sharing

Trusted Thin Client®



Key Benefits Include:

- DoD Grade Security
- NIST 800-53 Compliant
- Secure Operating System
- Open, Flexible Architecture
- Prevents Data "Leakage"
- Graphical-based Administration
- Supports LAN/WAN Configurations
- Mitigates APT with Virtualization
- Network and Data Isolation
- Reduces Operational Infrastructure (hardware, wiring, power, cooling)
- Lower Cost of Ownership

Raytheon
Trusted Computer Solutions
www.TrustedCS.com

"The threats posed by the modern computing environment cannot be addressed without support from secure operating systems. Any security effort which ignores this fact can only result in a fortress built upon sand."

– National Security Agency Report: The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments

Re-provision Existing PCs

RTCS can provide a firmware load that will take over the operating system of an existing PC and relegate that to "Smart Terminal" status. From that point on, it is similar in operations to a thin client computer.

RTCS also provides a USB fob that is bootable. This can be loaded onto a traditional PC and booted up. When booted, the only operating system accessible is on the USB and it can provide a secure connection back to the servers.

Production Ready with MLS capabilities

RTCS TTC is presently deployed in a number of DoD agencies and across the US Intelligence Community. It can host up to 8 desktops on a single trusted computer. Each of these desktops can run across a different network. Deployments have included JWICS, NIPRNET, SIPRNET and local agency networks. No data can be moved between networks unless a higher level utility is deployed. Operations, such as cut and paste, are disabled when attempting to be executed across networks.

Displays and Graphic Windowing

Each TTC can support multiple display screens as noted in the diagram above. There is no correlation of displays to desktops. A single desktop window can go across all displays (there is a video demonstration of this capability). Multiple windows of multiple desktops can be spread across all or a subset of the displays. Each window image has a border identifying the network/desktop it is hosting. Only content from the same desktop may be cut and pasted between similar windows. Additional products are available from RTCS to enable other operations to move data between desktop images by an authorized user.

The Smart Terminal Control Unit

Just as the original 3270 dumb terminals had a control unit that tied multiple devices to a network concentrator and then provided a connection to the mainframe, the same capability is required for the Smart Terminal. The Smart Terminal Control Unit is a security boundary appliance (physical or virtual) that redirects client content from the applications at each network level directly to the clients, while providing necessary security protections to maintain domain separation. Security protections, including the trusted operating system, prevent data from being transferred between security levels.

Using the previous finance trader example, the Internet can be connected so that consumers can contact the trader and an intranet can be deployed for the trader to access internal systems from which they can make a trade.

This Smart Terminal control unit acts as a network concentrator and can reduce the amount of cabling necessary for each end user. Each Smart Terminal control unit can manage 250 trusted thin clients. This simplification also reduces the security risks and intrusion points on the network. This capability is delivered by RTCS.

Certification and Accreditation (C&A)
SOTTC is engineered to satisfy cross domain security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) C&A processes. RTCS products are installed and accredited in operational systems around the world.

Virtual Desktop at the Server

Virtual Bridges' VERDE offering provides a number of benefits toward management of the virtual desktop image.

Golden Master Desktop Images

VERDE provides a centrally managed facility to create golden master desktop images. These can be any x86 based operating system image. Customers have built images for a variety of Microsoft Windows OS versions and Linux images from different distributors. In addition, the OS images may have different middleware loaded onto them (e.g. web browsers, office suites). All patches and software deployments are executed from a central administration portal. Software updates are automatically deployed with each boot up. System images are cached in the file system to provide faster access and sharing across the desktop community. Typically, a business or agency might have about 5 master images, but customers have had up to 15. In this particular bid, more images are possible. Each image requires approximately 20 Gb of storage at the server.

User Support

Different users have different needs. As such, processing power on the server needs to be reserved for the different types of users. The following table shows some of the different deployment models and resource utilization that might be required.

Device Support

In the table below are a wide variety of Access End Points. The full MLS capability that is described in the Smart Terminal section is only accessible via an x86 hosted device. VERDE will support tablets and Smartphones directly, but the MLS functionality of the RTCS TTC device is not yet available toward those devices.

	Task	Knowledge	Power
Workloads	▪ Call Center ▪ Transactional ▪ Lite Desktop User	▪ Office ▪ LOB	▪ High Performance Desktop ▪ Multimedia ▪ Design
Access End Point Device	▪ Repurposed Desktops ▪ Thin Clients ▪ Kiosks ▪ Remote Branch VDI, Online VDI	▪ Desktops ▪ iPads ▪ Laptops ▪ Station Access Points (e.g. Nurses Stations) ▪ Remote Branch VDI, Integrated Offline VDI, Online VDI	▪ High-end Desktops/ Workstations ▪ Power Laptops ▪ High Mobility (executive travel) ▪ Integrated Offline VDI, Remote Branch VDI, Online VDI
Scaling Considerations	▪ Up to ~16 Conconurrent Virtual Desktops/Server Processor Core	▪ Up to ~12 Concurrent Virtual Desktops/Server Processor Core	▪ Up to ~8 Concurrent Virtual Desktops/Server Processor Core
Memory Configurations	▪ Per Desktop ▪ Linux: 512MB ▪ Win7/XP: 512MB	▪ Per Desktop ▪ Linux: 512MB ▪ Win7/XP: 1GB	▪ Per Desktop ▪ Linux: 1GB ▪ Win7/XP: 1-2GB
Remote Protocol Considerations	▪ RDP, Nx	▪ RDP, Nx, SPICE	▪ SPICE

lsantalucia@vicominfinity.com

For the Power and Laptop users, if a full desktop OS image is required, VERDE can manage and deploy those images remotely to eliminate the need for end user responsibility in patch management.

Remote Protocol Support

RDP and VNC are supported by VERDE and TTC. SPICE is supported by VERDE and is presently under development for the RTCS TTC. It should be available in time for Air Force product deployment.

Secure and Resilient Desktop Consolidation Hosting Service

So far, we've replaced the PC with a Smart Terminal that is a stateless machine, so where do the brains of the operation reside? The initial deployment of RTCS Trusted Thin Clients was on blade servers that would be dedicated to a particular labeled compartment. Using the financial markets trader, the PC's associated with internet access would be consolidated on a set of blade servers for that function and the internal trading PC's would be consolidated on a different set of blade servers. With a ratio of about 3-8 desktops per core, 8 cores per blade and 14 blades per blade server, close to 600 PC's might be consolidated into one blade server. With compartmentalization, redundancy and thousands of end users, many blade servers would be required to meet the needs of the business or agency.

IBM has introduced the zEnterprise Bladecenter Extension (zBX) as a pre-built, fault avoiding host environment for Power and Intel blades. For STASH, the IBM eX5 blades can be deployed with 16 cores and 28 blades per zBX. Up to four zBX racks can be deployed per System z server. Approximately 3500 "desktops" can be operated within an individual zBX rack.

The goal of zBX is to run the desktop workloads on the blades while the security and management environment is provided within the System z server. In addition, database and application server workloads can be run within System z operating systems. IBM's System z is capable of operating thousands of virtual PC images in a single physical server, while maintaining separate compartmentalization domains across these PC images. Energy and floor space are conserved with this approach. The desktops can now operate at close to fault tolerant due to System z hardware architecture redundancy and automated operations to provide backups and hot standby PC image processing. The System z architecture also has a number of built in security features that further reduce risk between the Smart Terminal, Smart Terminal Control Unit and the PC hosting environment. This simplification of operations provides fewer points of control, fewer points of intrusion, fewer points of failure and reduced cost of deployment over alternative deployment models.

Management Server

The System z Enterprise Linux Server (ELS) provides the hosting environment for most of the management server capabilities. It is a fault tolerant/fault avoiding server platform that is capable of running at 100% utilization at all times, without fear of failover. Depending on the server model deployed, the processor speed executes at either 4.4 Ghz or 5.2 Ghz. This enables massive scaling of images and transactions per second as compared to x86 server cores.

Security Server

The ELS utilizes an LDAP server that can also leverage IBM's RACF Security server in the roles of identification, authentication and access control of end users. These servers support the deployment of DoD Smartcards for desktop authentication services and other x.509 certificates.

The ELS server itself provides military grade MLS capabilities and has been certified by the US Intelligence Community and through evaluation of the Common Criteria international standards for high assurance platforms.

Blade Server Management and Connectivity

Between the zBX and ELS are two networks. One is a direct 10 Gb Ethernet connection for interoperability. This can include access to the storage area network and management servers. The other network is 1 Gb used to manage the physical and virtualization attributes of the blade servers in conjunction with the ELS. The System z Unified Resource Manager (zManager) provides an end-to-end management service to start/stop blade virtual machines, collect performance information to enable add and subtraction of blades as necessary based on the workload and to manage the electricity and cooling of the zBX racks. In addition, it provides a call home capability should any hardware component in either the ELS or zBX fail. This call can go to the IBM support services so that a Customer Engineer can be dispatched immediately to correct the situation. Because of the redundant hardware components deployed, many times, the servers can continue operating with the failing part. The mean time between failure of ELS far exceeds that of traditional x86 environments with a goal of zero unplanned outages.

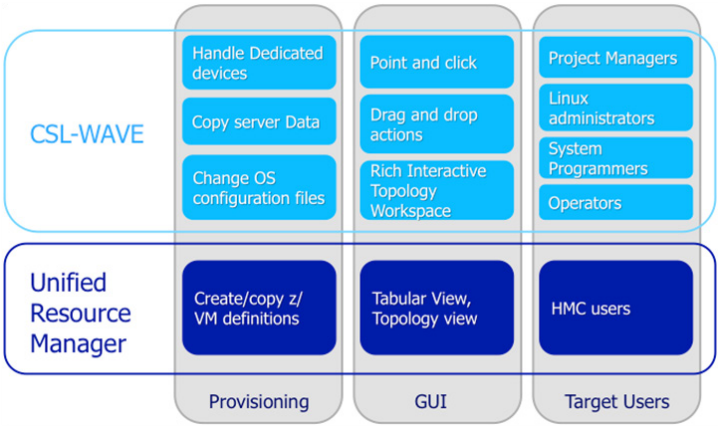
Virtualization Management Redefined

The blades utilize the KVM server as the means of virtualizing desktop images. On top of this, a product called the System z Unified Resource Manager (zManager) is deployed to centrally manage the virtualized images. VERDE, which supports KVM, VMWare, Hyper-V and Xen virtualization platforms is working with IBM to ensure its' desktop management supports the URM api's which simplify the deployment and management of virtual machines.

With so many PC's concentrated into one secure and resilient physical server, it could be a very complex operational environment, but it really doesn't have to be. Separate logical partitions can be established for each compartment or domain in which the organization wishes to operate similar PC security domains. These logical partitions and the virtual machines within them can be managed on System z196 and later systems by the recently introduced System z Unified Resource Manager or zManager for short. This provides a high-level management structure for provisioning individual virtual machines. This is akin to making a purchase order for a new PC and making this new machine available to the end user.

CSL International developed their CSL-WAVE offering to manage the operating system and workloads within those operating systems on top of the virtual machines. Working in conjunction with zManager, they provide a simplified GUI interface that manages, clones and maintains service level agreements for the applications running within the z/VM virtual guest systems, which in this case would be the Linux and Windows operating systems running on top of z86VM.

CSL-WAVE and zManager greatly simplify the management of thousands of Smart Terminals hosted across multiple z/VM system images. They CSL-WAVE and zManager greatly simplify the management of thousands of Smart Terminals hosted across multiple z/VM system images. They work closely with the guest operating system, z/VM hypervisor and System z hardware to maintain capacity/utilization agreements, security and resilience of the Smart Terminal workloads.



"(we) started implementing Linux on System z in 2009. Our first production system went live in October 2009. We currently have approx. 20 production images with ten more in test/development.

CSL-WAVE has been with us from the start. Its capabilities facilitate the rapid deployment of new Linux images. It ensures that all new images conform with the Best Practices we have decided to implement.

As an operations tool, it allows our distributed operations staff (who know nothing about z/VM and very little Linux) to manage our systems through its friendly GUI.

CSL as a company provides top-notch support. They are always responsive to new requests, enhancements and ideas."

High Availability, Disaster Recovery and Coop Sites

The ELS server can be connected to up to three other ELS servers to operate as a single system image for the management servers running within it. Should any component fail, new requests will be redirected to other server images. In addition, the ELS provides live guest relocation (LGR) of server images across this single system image as another mechanism to avoid system down time.

Each ELS server can also globally mirror its data (both local and storage area network) to a hot site that can be greater than 100km away. Standby servers can be acquired for a fraction of the cost of a production server. These are called Capacity BackUp (CBU) processors. These discounted processors can be installed in another production ELS server or in a separate ELS server dedicated to backup processing. There are no software license fees associated with these servers as the licenses will transfer from production to backup when the recovery action occurs. This can result in significant savings over x86 server deployments, which include fully paid hardware and software licenses for backup processors.

Performance Monitoring

The STASH solution includes deployment of Tivoli Omegamon Performance Monitoring for both ELS and zBX workloads.

Storage Management

The STASH solution uses IBM VS7000 FCP deployed storage area network. This storage can be locally attached to the ELS to meet the needs of the management server images and NAS attached to the desktop images to satisfy both the Global master images and the individual user images. Typically, 16 Gb per user is defined for their personal usage. This can easily be configured and managed through the VERDE solution at the desktop user. For the management servers, the deployment will be controlled by the WAVE offering.

For each ELS, a Virtual Tape Server will also be deployed for backup/restoration services. For remotely managed ELS, this recovery action can occur remotely.

Network Utilization and Management

The combination of CSL Wave and zManager will manage the network topology between the x86 blades, hosted on the zBX and the Enterprise Linux Server. There are several phenomena at play that concern network utilization. A physical desktop may regularly interoperate with other systems, such as through interactive support (e.g. HTTP, 3270, telnet

.

Scalability

Up to four zBX racks can be attached to a single ELS. That shows that between 14,000 and 28,000 desktops can be managed within a single ELS server. With the single system image support of ELS enabling up to four ELS servers to be clustered together, 56,000 to 128,000 desktops can be managed in a single system image. Lastly, each of the ELS servers can be remotely managed. For example, there is one retail operation that has 49 remote servers managed from their headquarters location. This includes software delivery, start, stop and monitoring of the servers.

Diverse Workload Management

Most organizations determine that they should only manage a single workload domain. In this case, this bid is only for Virtual Desktop capabilities. Part of the reason that virtualization of desktops is successful is because a single desktop's compute resource is only utilized for a

lsantalucia@vicominfinity.com

fraction of its computational capabilities. Standalone desktops may only use 5% of their compute resources while the remaining processing time stands idle. In a virtualized blade environment, up to 50% of the processor power may be utilized. The rest remains idle to handle spikes. However, if this processor power is only consumed for desktops, then that capacity may be underutilized off-shift, when the majority of users are at home. Now in this Air Force bid, it is assumed that processing occurs around the globe so depending on network connectivity, capacity may be spread across a larger number of users, but at different times of day. As a result, fewer server images may be deployed.

But where the compute processing is locally deployed for the desktops, it may still stand idle off shift. With the use of zManager, this idle time can be consumed by other CPU intensive workloads. For example, one customer suggested that the STASH solution could provide "desktops by day and analytics by night". Stated more generically, it could be "desktops by day and enterprise servers by night". Executing in this environment would require additional configuration and storage. However, the management solution and processing power is already going to be on the floor. As mentioned earlier, VERDE provides golden masters for desktop images and CSL provides golden masters of ELS server images. CSL presently has in development the support of golden master server images for x86 hypervisors via both the libvert() api and the URM api's for the zBX hosted environment. Using CSL Wave, both desktop and server images can be deployed across the zBX blades and managed to capacity goals as defined in service level agreements. In essence, the STASH environment can operate as a fully utilized Cloud or Grid for deploying both desktop and server workloads. This can dramatically reduce the number of physical servers deployed, as well as the energy and intranet networking required to satisfy these diverse workloads. This blade virtualization server management offering is expected to be available in 2Q2012.

Risk Mitigation and Fraud Prevention

Each end user has the ability to access resources within the various network domains that they are connected to. Typically, logs are kept to look at transaction updates. Other logs for browsing data can be created through other products such as Guardium. The STASH offering includes Intellinx' zWatch which provides a unique User Activity Monitor that captures network traffic generated by an end user over a wide variety of popular formats and protocols. Consider this a Digital Video Recorder (DVR) of end users. It can be implemented so it is using an asynchronous network path to eliminate any impact on the end user performance. It can also provide synchronous workflow support to solicit additional approvals before an access is executed. These protocols include 3270, HTTP, Telnet, SSH, MQ, Web service, and several distributed database protocols (e.g. Microsoft SQLServer, IBM DB2 and Oracle). The formats and protocols are reverse engineered to save data as fields for subsequent searching and investigative services. This saves storage space and processing time. This product is deployed in production at NY Police Dept, Delaware Criminal Justice System, and Bureau of Prisons within the Justice Dept. to name a few agencies. It is also deployed across financial services and health organizations to ensure that the privacy of personally identifiable information is protected. This product can be deployed by itself or as complimentory alert capabilities to other SIEM offerings. The most important feature is the ability to look across systems and recreate end user activities to determine intent of the individual in accessing information. This has been the most valuable use of the technology. Other products tend to analyze one server or function at a time and manual intervention may be necessary to correlate events across multiple systems, whose windows are open simultaneously on a desktop.

Remote Administration

The combination of Enterprise Linux Servers and CSL-WAVE enable remote management of the configuration. There is a large customer today with up to 50 remote systems, all managed from a headquarters location. The remote systems are considered "fault tolerant" in the local deployment. While all these systems are physically located, but geographically dispersed across North America, there is no reason that this can't be done on a global scale. Many customers have several systems, globally deployed, but managed from a central location.

Comparison of Acquisition Costs

The STASH solution is roughly comparable, in price, to an x86 virtualization environment. The key is to look at the aggregate capital costs of the entire infrastructure vs. looking at the individual pieces. The trusted thin clients, when used in a single network, are about the same price as other thin clients and less expensive than desktop upgrades to a stand alone PC. When multiple desktops are consolidated onto a single trusted thin client, the TTC is a much cheaper solution.

The aggregation of desktop virtual machines on zBX racks with the associated management and security on System z virtual machines is about the same cost as x86 virtual machines.

The largest difference in capability is the addition of the Intellinx Fraud Solution and CSL Guest management. These are additional functions that might not be included in a "strict" virtual machine deployment strategy on x86.

When the cost of the entire solution is then divided by the number of desktops being hosted, the cost per seat will be comparable to alternative thin clients and less expensive than a PC upgrade.

Deployment and Payment Models

There are several deployment models to choose from, each having different pricings models.

1. Customer acquires new hardware, owns and operates the deployment of both the desktops and servers necessary to launch a VDI program. This price may range between $500 to $1700 per seat, for all new equipment (desktop and servers). This price would include hardware, software and maintenance over a three year period. Seat price varies between general office usage (about 16 desktops per core) and power users (8 desktops per core). Volume discounts are possible. These prices don't include installation and customization fees as this amount will vary based on the number of systems deployed.

2. Customer acquires only the equipment that it needs. This includes re-provisioning existing PC's as thin clients (to avoid thin client hardware acquisition) and leveraging existing blades and Enterprise Linux servers to host systems. Pricing will vary based on the number of reusable components.
3. Customer could contract out the desktop servers as a Cloud offering. This price has not yet been established.

Optional Value Added Services

Certificate Authority

Some customers utilize IBM z/OS for some of their high scale transaction processing. z/OS provides a Certificate Authority (CA) within its RACF Security server. Several governments have leveraged the Certificate Authority within RACF to support up to 12,000,000 individuals with unique digital certificates. These certs can be provisioned at no charge to end users vs. leveraging a third party CA that might charge up to $2 per cert. These businesses have experienced tremendous savings in third party license charges while meeting the demands of their end users. The processing power of a CA on z/OS is very low as this capability is typically utilized only on sign on. In addition, all the benefits of z/OS fault avoidance are available through this offering.

Application and Data Integration With Desktops

No desktop operates as an island, though many businesses and agencies may operate them separately. As mentioned, many customers leverage System z in their operations today. Rather than deploy new System z114 images for the sole purpose of managing desktops, zBX racks can be added to existing zEnterprise servers to reduce some of the deployment costs. In addition, any applications residing on the zEnterprise servers can leverage the direct interconnect to the zBX to further reduce intranet bandwidth and protect against sniffing the network internally by rogue users. The zBX is also capable of hosting Power blades for the AIX operating system. Where capacity allows, some of those workloads could be deployed on this same direct connect networking fabric and be managed by zManager to further reduce operational complexity, simplify security and resilience and reduce overall costs of operations.

Smarter Buildings: Networking, Environmentals – Space, Energy, Cooling

- When desktop PCs are replaced by a trusted thin client, there is a reduction in energy usage.
- When multiple desktops are consolidated into a single trusted thin client, there is a further reduction in energy, a reduction in network wiring and a reduction in network bandwidth.
- Physical servers take floor space, electricity and cooling. System z's ability to consolidate many x86 system images or functionality into a System zEnterprise can dramatically reduce the environmental costs.
- When desktops are leveraging mainframe data and applications, there is a dramatic reduction in networking bandwidth required within the intranet as a direct connection is provided between zBX and System z servers.

Performance Disclaimer
All performance data contained in this publication was obtained in the specific operating environment and under the conditions described below and is presented as an illustration. Performance obtained in other operating environments might vary and customers should conduct their own testing. The information contained in this document is distributed AS IS, without warranty of any kind. This document applies to Trusted Thin Client®, CSL-WAVE, Virtual Bridges VERDE , Intellinx zWatch and System z.

For further information contact:
Len Santalucia
CTO & Business Development Manager
STASH Consortium
One Penn Plaza - Suite 2010
New York, NY 10119
212.799.9375 o
917.856.4493 m

lsantalucia@vicominfinity.com

STASH Consortium